Yuval Ne'eman Workshop
for Science, Technology and Security
Tel Aviv University

ICRC
Blavatnik Interdisciplinary
Cyber Research Center

Prime Minister's Office
National Cyber Directorate

The Blavatnik Interdisciplinary Cyber Research Center
Yuval Ne'eman Workshop for Science, Technology and Security
Tel Aviv University

The Annual Cyber Security International Conference Proceedings

Cyber Week 2016

TEL AVIV UNIVERSITY
אוניברסיטת תל אביב

Yuval Ne'eman Workshop
for Science, Technology and Security
Tel Aviv University

ICRC
Blavatnik Interdisciplinary
Cyber Research Center

Prime Minister's Office
National Cyber Directorate

THE 6TH ANNUAL CYBER SECURITY INTERNATIONAL CONFERENCE PROCEEDINGS

Cyber Week 2016

THE YUVAL NE'EMAN WORKSHOP
FOR SCIENCE, TECHNOLOGY AND SECURITY

THE BLAVATNIK INTERDISCIPLINARY
CYBER RESEARCH CENTER

MAY 2017

TEL AVIV UNIVERSITY
אוניברסיטת תל אביב

THE ANNUAL CYBER SECURITY INTERNATIONAL CONFERENCE PROCEEDINGS 2016

The Annual International Cybersecurity Conference is held by the Blavatnik Interdisciplinary Cyber Research Center (ICRC), Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University and the Israeli National Cyber Bureau, Prime Minister Office.

With each passing year the conference grows as the awareness of the increasing threats becoming a matter of international concern and common knowledge. Israel, known as the start-up nation, is now becoming a cyber-nation, one which combines high-end technology, innovation and the talented innovators. The conference will include speakers and delegations from both Israel and abroad who will share their insights on the most recent developments in cybersecurity and discuss key dilemmas and opportunities arising from the evolving technologies.

The conference receives extensive global media coverage. The last conference enjoyed the presence of more than 5,000 attendees from 48 countries. Attendees included: decision makers, diplomats, academics, respected members of the defense industry and intelligence units, Israeli and international students, hi-tech entrepreneurs, leading experts from the cyber industry, cyber professionals, corporate C-suite executives and senior decision makers representing policy circles, the private sector and defense in Israel and abroad.

YUVAL NE'EMAN WORKSHOP FOR SCIENCE, TECHNOLOGY AND SECURITY OFFICIALS:

Major Gen. (Ret.) Prof. Isaac Ben Israel, Head of the Workshop
Mrs. Gili Drob – Heistein, Executive Director of the Workshop
Ms. Revital Yaron
Mrs. Roni Sharir
Mrs. Dafna Kovler
Mrs. Liana Rubin

Editor: Yael Luxman-Bahat
Technical editor and professional advisor: Yul Bahat
Graphic Editing: Michal Semo Kovetz
Printed by: Tel Aviv University Press, Israel, 2017

The Blavatnik Interdisciplinary Cyber Research Center (ICRC) was established at the Tel Aviv University on April 2014, as a joint initiative with the National Cyber Bureau, Prime Minister's Office. The Center is based on researchers from Tel-Aviv university and emphasizes the importance of interdisciplinary research. Currently, there are 50 faculty members and over 200 cyber researchers from different faculties such as Exact Sciences, Computer Sciences, Law, Engineering, Social Sciences, Management and Humanities.

The Center aims to become a leading international body in its field and to increase the academic efforts and awareness in the field of cyber security. Research topics at the Center include key issues such as security software, attacks on hardware and software, cryptography, network protocols, security of operating systems, and networks as well as interdisciplinary research such as the impact on national security, the impact on society, regulation, and the effects on the business sector.

The Center operates a research fund which is supported by the Israeli National Cyber Bureau, Prime Minister's Office.

The Yuval Ne'eman Workshop for Science, Technology and Security was launched in 2002 by Major-General (Res.) Prof. Isaac Ben-Israel in conjunction with the Harold Hartog School of Policy and Government and the Security Studies Program at Tel Aviv University. The Workshop was founded with the clear directive of exploring the links between science, technology and security. The Workshop conducts a broad range of research activities that include the publication of research papers and policy reports in the field of national security strategy & policy. Alongside its research activities, the Workshop also holds a senior executive forum that promotes public-private partnerships and initiatives and a popular series of monthly conferences at Tel Aviv University with the participation of senior IDF staff and security organization members, politicians, academia, and executives from leading Israeli and International companies. The goal of the Workshops' activities is to create an open and fruitful dialogue with the general public in the fields of interest of the Workshop: Cyber Security, Space and Emerging Issues of National Security.

CONTENTS

PREFACE

Cybersecurity is about restricting the dark side of computer technology: by putting computer chips everywhere, we create a weak point that can be used by "bad guys" to harm our society. Cybersecurity is about solving these problems. However, although cyber problems usually have technical solutions, the problems are never purely technological. Social behavior, legal aspects, business consideration etc., all play a large role in understanding the "problems". Hence, cybersecurity is interdisciplinary by its very nature.

The Blavatnik Interdisciplinary Cyber Research Center (ICRC) at Tel Aviv University, has established itself as Israel's focal point of interdisciplinary academic cybersecurity research, innovation, entrepreneurship and policy initiatives. One outstanding example is the center's advancement of public-private partnerships by holding a senior executive forum with the participation of defence officials, politicians, business leaders and scholars from leading Israeli and international entities. We also warmly welcome international cooperation, which has, in recent years, given our research and policy activities global exposure and recognition, and has also helped to sustain the Workshop's growth.

The Annual Cyber Security International Conference at Tel Aviv University has showcased our work since 2011. It's my hope that the research and policy presentations included in the following Proceedings will interest you and deepen your understanding of key issues. The presentations here give diverse views on cybersecurity by ministers, key government actors, leading enterprises and academics from Israel and around the globe. Those of us who have participated in the ICRC's past conferences have benefited from cutting-edge insights.

May the materials included here indeed contribute to deeper understanding, and to a more prosperous and more secure future for Israel and for the world.

Prof. Maj. Gen. (Ret.) Isaac Ben-Israel

Director of the Blavatnik Interdisciplinary Cyber Research Center (ICRC)
Head of Yuval Ne'eman Workshop for Science, Technology and Security
Tel Aviv University

FIRST ASSEMBLY

OPENING REMARKS

DR. EVIATAR MATANIA, HEAD OF THE ISRAEL NATIONAL CYBER DIRECTORATE, PRIME MINSTER'S OFFICE

I am going to talk about a five-year perspective on cyber. Usually one should be quite careful when talking about a five-year vision or forecast, so what I will do is the easier thing – I will talk about those five years backwards and then to try and address how I see the real challenges in the coming five years ahead, not to try and forecast but to put the challenges in front of us.

Usually a phenomenon, such as the cyber, has a starting point that one could look at and say "here this phenomenon started", but it is quite difficult to find such a point. It is, however, easier to find the focal point, where the changes became dramatic. I think that the focal point of cyber was Stuxnet in 2010. I think that the focal point of understanding the cyber threat was approximately five years ago, and this point changed the way the top executives and decision makers thought about cyber. Before that point, the cyber threat and the cyber issue in general were usually under the responsibility of the IT managers, but five years ago top executives in organizations, federal administrations, and governments, started realizing that the issue is much bigger than the mere responsibility of CISOs or IT managers.

Since then, the idea had spread all around the world, to the point where nation-states form and structure new strategies in order to mitigate the cyber threat, and most nations are doing something to develop new technologies in order to address this threat. I believe what happened during the last five years is the development of an idea. Take Israel as an example; five years ago, here in this podium,

our prime minister stood here and drew a vision of how Israel should approach the cyber phenomena and the cyber domain. I was sitting here, and had no idea that in several months I will be called by the prime minister to take his vision and the governmental resolutions and to implement them into something real and vivid.

In these last five years, we dealt with many ideas, we developed our strategies, we planned how to structure our way of addressing the threat. We invested a lot in technology, approximately $100M in programs to encourage our new scientists and our young generation to come and work in the cyber domain. We have a lot of programs, some of them together with the Tel Aviv university, to train young people, starting at the age of fourteen, to be cyber experts. We invested a lot in our universities, establishing five new research centers for cyber security. We invested, together with our colleagues in the Ministry of Economy, Ministry of Science, Ministry of Education and in our industry, and we developed strategies which I believe are the most advanced strategies for addressing the cyber threat.

I think I can point towards a focal point that took place in the last year – a point where you can see, all around the world, that ideas are turning into actions. Again, I will use the Israeli example: over the last year we have established the new cyber security authority, and were perhaps the first in the world to establish a new structure in order to address the cyber threat; and in January we have nominated my friend, colleague and partner, Mr. Buki Carmeli, as head of this authority, and he started working in April. Also, over the last year we have established fifteen new units in different ministries in the government, in order to tackle the cyber threat, and we nominated many people in the government to be responsible for the cyber risk in the ministries; we succeeded to take the idea of the cyber city Beer Sheeva into real action, and there are companies that already benefit from our exempts there. We took ideas and put them into actions.

I think that this year we are at another focal point, and that we will see all around the world that ideas are turning into actions. If we stand here in five years, I believe we will see that by then most of the countries will adopt new structures. We are the first to do so; I know that the United Kingdom and Singapore have a new authority, but soon you will see all around the world – new structures, new ideas and new technologies that are going to tackle the cyber threat. And I

believe that this structure, and the new technological breakthroughs, will change the current unbalanced equation between attackers and defenders.

Currently I think that the equation in the cyber domain is not balanced. We are too vulnerable. But I believe that in five years, if we see all around us nations adopting new strategies and technologies, this equation will become much more balanced. From my point of view, through a five-year perspective of cyber, during the five last years we moved from ideas into actions, and during the coming five years we are going to see those actions structure technologies all around us.

To summarize, from a five-year perspective I think we are currently in the focal point of turning ideas into actions, and that this conference gives us an opportunity to discuss how we take the ideas into actions, and how we make it easier for nation-states to adopt new structures and technologies, and to encourage everyone around us – organizations, governments, and others – to join us in making the dark side of the moon much more brighter.

ALEJANDRO N. MAYORKAS, DEPUTY SECRETARY OF HOMELAND SECURITY, USA

I would like to share a few thoughts about the landscape in the United States domestically in terms of our federal governments efforts, speak a bit about the international euphoria in which we operate to address our cyber security challenges, and then to share with you what I deem to be imperative for the future. In the United States, the federal government is in the process of reorganizing itself to best meet the cyber security challenges that we confront. To that end, the department of Homeland Security has been placed in the point position – the tip of the spear, if you will – on behalf of the federal government. We do not only drive the security of federal government departments and agencies throughout the administration, but we are also the point in a public-private partnership, that ensures that the federal government and the private sector work together to address a challenge that confronts us both.

In this regard, one of the edifices or institutions that we are developing is the architecture of information sharing, and the second one is a response protocol unique to the cyber security challenge. In normal

criminal law, the focus of attention on behalf of a government is the identification and apprehension of the perpetrator, to address the threat in the first instance. In the cyber security realm, we recognize that the identification and apprehension of the perpetrator can be very difficult – the perpetrator could be on the other side of the globe, as we know cyber security knows no boundaries. Therefore, it is critically necessary to ensure that we exfiltrate the harm, remediate and repair it. The ability to protect the asset in the cyber security realm can be more important than the apprehension of the wrongdoer.

Between those two architectures, the sharing of information and the response to the asset that is the target of a cyber security challenge, we are building a new culture and a new institution in the federal government. In doing so, we confront challenges, some of them in the area of information sharing between the private and the public sectors.

First, at a very nascent stage, industry individuals and companies ask us: what is the benefit for us to share information? And the answer is, in one of the unique natures of the cyber crime, the ease of replication; just as a perpetrator victimizes one individual computer or one institution system, that harm can be replicated with ease and with tremendous speed. In this manner, the ability to share information with the government so that it, in its unique position, can disseminate the cyber threat information to others throughout the country, will ensure that the replication of the harm never materializes. Therefore, even though we are at a nascent stage of this information sharing architecture, I am confident – because of our abilities and the capabilities that we are developing – that we will indeed instill this culture in the private and the public sector.

The second obstacle that we confront is the issue of trust. There is still a chasm of distrust between the private sector and the federal government. I personally believe that to some extent, as the federal government, and certainly in the cyber space, we are still operating in the shadow of the Snowden disclosures several years ago. When an individual or an institution shares information with the government, the question is what will the government do with it, and the legislation that the Congress implemented in 2014 and the policies implemented since that critical piece of legislation provides adequate protection in that regard.

In addition, there is a concern about accountability. Some of our independent regulatory agencies have brought actions against institutions when those institutions revealed inadequate cyber security processes to protect shareholders, customers and consumers more broadly. The accountability regime in our country serves as a point of hesitation in an institution's willingness to share information with us. Of course, there is also the issue of civil liability – not just government action but consumer litigation, should the information provided reveal a level of negligence. This too the legislation and our policies have guarded against. There is anonymity if one so chooses when one wants to provide information to the government; there is liability protection; and there is the confidentiality of the information once we, in the department of Homeland Security, receive it.

I think that our ability, our unique position to receive information and to disseminate it broadly, is a galvanizing force in the information sharing architecture, which we see as critical to the future. There is one element to it, from a market perspective, that I would implore people to embrace, and that is the notion of a public good. The cyber threat indicator itself is now a commodity that is a value in the marketplace. The cyber security industry has blossomed and grown so significantly, beyond the mere possession and dissemination of the cyber threat indicator, that that indicator need no longer be treated as a commodity, and should be treated as a public good. If we share the cyber threat indicators with one another, we can achieve the goal that I previously articulated – to ensure that our vulnerability, once discovered, is not twice exploited. If one institution is victimized, and it shares that vulnerability with others, let us be sure that the second and subsequent institutions that share that vulnerability are not similarly victimized. We must share information, and specifically the cyber threat indicator, to achieve that result.

One of the lessons that we have experienced in the cyber security world is that to go it alone is a very precarious endeavor, but working together makes us all stronger and creates an ecosystem that will best protect us.

That leads me to turn to the international arena. We enjoy an extraordinary close partnership with the state of Israel; we have reached agreements in the past and will continue to do so in the near future, to embark on an automated information sharing protocol together.

This is a capability that we in the department of Homeland Security have developed, the ability to receive information in automated form and to disseminate it in near real-time in automated form as well. I say in "near real-time" because critically I spoke of the confidentiality provisions and the ability to protect privacy interest, and that we are able to do it in seconds and minutes.

The cyber security threat is borderless, so just as we are changing information sharing domestically, we are changing it in the international arena as well. Information must be shared between and amongst countries, through their computer emergency response themes in CERT-to-CERT relationships, and otherwise. We must also ensure that countries follow the well-established international norms. We are pleased that we were able to negotiate an agreement with the republic of China to ensure that it abided by the international norms, and critically the norm that it will not engage in cyber conduct to steal secrets for the commercial advantage of entities operating in it's domain.

With respect to cooperation, there is a critical need to share our research and development, as well as our innovations, and in that regard the United States and Israel also share a very strong bond and a very strong partnership. The United States, with our remarkable resources, our technological innovation, and the dynamism of our tech community, can certainly be a leader in cyber security across the globe. Israel, a much smaller country, can be and is our close partner and great ally; and I think that it is because of a number of unique reasons, not just its extraordinary brilliant individuals working not only in universities and in government, but in the private sector, in close partnership with those institutions, but also because of the architecture developed by Dr. Eviatar Matania. It is an extraordinarily high priority of the Prime Minister and the government as a whole, to ensure that the cyber security of the nation is a result of tremendous investment of talent and funds. The cyber security authority reports directly to the Prime Minister, which reflects the prioritization of this critical agenda.

It is also Israel's position in the world as a cyber security leader, and we can all benefit from following the model of Israel and listening and adhering to the vision of some of its leaders.

The tech industry in Israel is growing by leaps and bounds, and it also has the unique ability to recruit talent through military service; through the identification of individuals with the talent needed to develop the cyber security of tomorrow. Israel, along with the United States and other nations, is poised to work as a collaborative partner to ensure that our united ecosystem is stronger today than it was before.

A question frequently asked is whether our security can keep pace with our technological innovations, and what we can do to make sure that the driverless car of tomorrow is secure given its reliance on technology. In my opinion, that tomorrow is already here today. We cannot think that tomorrow is too far away when we speak of the need to ensure that security keeps pace with technological innovation. That tomorrow is here, and we are all gathered here today because of that reality. We all need to work together to make each of us stronger and more secure.

MK AYELET SHAKED, MINISTER OF JUSTICE, ISRAEL

It is a pleasure for me to take part in the evolving discussion on one of the most challenging policy issues democratic governments deal with today – how to secure cyber space while maintaining its open innovative nature.

As minister of justice, I feel a heavy responsibility in promoting a legal framework for a secure cyber environment; at the same time, as a computer engineer by training and former member of the high-tech community, I am deeply committed to preserving the spirit of technological innovation that drives our society, and minimize regulations and controls.

When I think about the rule of law in cyber space I understand the need to bridge the gap between law, which embodies our values and ideas, and the technological reality. The challenges the democratic states face today call us to action, action in which lawyers, policy maker and technologists come together – much like in this conference – to discuss and develop the next generation of legal norms for the 21st century.

First, I would like to discuss the risks and challenges from the government's perspective. A few years ago, some leading figures spoke about cyber Armageddon, but the threat assessment has changed in recent years. In remarks he made in 2015 to the Senate's Armed

Service committee, James Clapper, director of National Intelligence in the US, said that while the threats of cyber Armageddon remains, we have been living with a constant and expanding barrage of cyber attacks for some time – cyber attacks from both state and non-state actors, including terror and cyber crime groups – from parts of this virtual front that states are being called upon to defend. I chose to use the word "front" and not "battlefield" because it is so much more complex than a traditional battlefield.

In this virtual front, the number of malicious actors, their technical capabilities, the scope of their attack methods, and their range of targets are constantly increasing. These threats undermine trust in cyber space as an open domain which enables the free flow of information, capital and services, promotes innovation and enhance overall welfare. Therefore, governments are called upon to step into what was traditionally viewed as a private playing field, and are compelled to invest resources in enhancing their cyber capabilities to confront these threats.

Today, as ever, Israel is determined to defend its cyber domain. Cyber defense obviously takes many forms, but what I would like to focus on the leading role that the Ministry of Justice plays, domestically and internationally. Our goal is to promote a modern legal environment, where security and innovation in cyber space go hand in hand, so that Israel can be not only a leader in technology, but also a leader in cyber security law.

First, I will discuss the international aspect of cyber law and policy. The fact that cyber space is global in nature, and that information flows across borders, challenges the traditional notions of how international law applies to cyber space. International law is rapidly evolving, and many international forums raise a variety of legal questions with very real implications.

From Israel's perspective, it is a given that international law applies to the cyber domain. At the same time, the international communities are seeking to better define how the existing international law applies to the questions that are raised from cyber attack. For example, the need to take effective measures against attacks by non-state actors, and the need to confront cyber terrorism at the international level. Israel is known to have significant expertise in this area, and we have

to contribute to the international dialogue. As such, the office of the Deputy Attorney General for international law within the Ministry of Justice takes an active part in advising the national cyber bureau on international law questions, as well as in practicing in some of the international forums. In my view, international law has to provide effective and realistic tools to enable states to defend themselves, and we are committed to taking a leading role in the international conversation.

Turning now to domestic legislation in the field of cyber security, one cornerstone of Israel's cyber security strategy adopted in 2015 is the need to improve the cooperation of the private and public sector in cyber defense. Cyber space is made up of public and private organizations and their networks, and much of the infrastructure and functions that governments aim to protect is operated to also be applied by the private sector, though the government needs to strongly engage with the private sector in order to carry out its role as provider of security and safety.

The ministry of justice is working closely with Israel's national cyber bureau to develop a new cyber security law. By defining a clear coherent legal framework to implement Israel's cyber security strategy, we can promote the secure and safe functioning of cyber space, and a vibrant online domain that will preserve the benefits we have reaped from this space in the last twenty years.

Another important pillar in the defense of cyber space is the field of law enforcement. Cyber crime and cyber terrorism pose numerous challenges, such as the ease with which malicious actors can attain anonymity and encrypt their communication. Another challenge is the cross-border aspect of cyber crime and cyber terrorism, which enables malicious actors to evade the jurisdiction of legislative and judicial authorities, making it difficult or even impossible to collect evidence abroad.

Finally, the decentralized and structured nature of cyber space services and platforms makes it difficult to stop prohibited activity and impose liability. Terrorist groups and organized crime take advantage of those features, and have been moving a substantial part of their activities online. Cyber crime today is the fastest growing criminal activity, and the economic damage it has caused surpasses any other criminal activities.

Cyber terrorism also poses a significant threat. Cyber space is used for incitement and radicalization, recruitment and communication between terrorists, and it is also a target to terror activities.

To handle these challenges, the Ministry of Justice has established in the last year, since I was appointed as Minister, a dedicated cyber crime and cyber terrorism department within the state attorney's office, dealing with the entire range of offenses, from online fraud to child pornography to cyber terrorism. One main focus is large internet companies' platforms and content providers, such as Google, Facebook, Twitter, and Microsoft. Democracies across the world are grappling with difficult questions regarding what kind of regulation should be applied to those companies while preserving the open nature of the internet.

Israel wants to maintain its leading position as a world-class high-tech hub, and I am a firm believer in removing regulatory obstacles, so that innovation and investment can continue to thrive here. At the same time, I think we need to acknowledge the fact that some very severe crimes are being conducted and inserted through those platforms, and that there should be some measures of accountability for internet companies regarding the illegal activities and content that is published through their services. There should be a cooperation mechanism with the government, so that the companies can deal with these types of content, at the very least, if they are notified that a crime is being committed through their platform.

The ministry of justice is taking a leading role in this course of action. For example, we are promoting cooperation with content providers, sensitizing them as to content that violates the Israeli law or the providers' term of service. We are also working on draft legislation, similar to what is being done in other countries. One law that will allow for judicial injunctions to order a removal of websites from search engines, such as websites that incite to terrorism, and one law that will limit access to search in websites, like websites that distribute child pornography. In each case, we are talking about content and websites that reach a particularly high threshold of criminal severity.

These are issues that I have personally raised with other Justice Ministers across the world. I have also established a committee to deal with the subject I care deeply about – cyber bullying and online

shaming. I should also mention that Israel has recently ratified the Budapest convention on cyber crime. This important instrument will assist Israeli law enforcement authorities in addressing some of the above mentioned cyber crime challenges.

To conclude, the Ministry of Justice is investing considerable resources in promoting a sound pinpointed and technologically-aware approach to cyber security regulation, in a manner that balances between different goals interest and consistent with democratic values. This brings me full cycle to my earlier point: law and innovation should not be seen as competing values, but as a mutually-converging interest. My hope is that throughout constructive dialogue, both domestically and abroad, we can ensure that the law remains a useful social tool to promote a safe society. Israel is a leader in cyber security technology and I believe that we are poised to become a leader in cyber security law as well.

ZHAO ZELIANG, DIRECTOR GENERAL, BUREAU OF CYBER SECURITY, CAC

Cyber security is a big challenge for us. Nowadays, information technology revolutions showcased by the internet have brought profound changes to the world, including economic and social progress in our countries. Like many other nations, the Chinese government attaches great importance to the internet development and related issues. Three years ago, in order to unify leadership and overall coordination of cyber security work across the whole country and accelerate the internet development, China established the Central Leading Group for Cyber Security and Informatization, headed by president Xi Jinping, as well as the Cyberspace Administration of China (CAC), which acts as executive office of the entire group.

In April 2016, President Xi Jinping personally chaired a symposium on Cyber security and informatization in Beijing, the first of its kind in China. In his speech at the symposium, President Xi Jinping presented our Chinese leadership's views and approaches regarding cyber security, laid down a blueprint of China's internet development, pointed out the direction for work, priorities, and the requirements. President Xi Jinping's speech embodies China's strategic framework and action plan for cyber security. It is also the best guiding document for the world to understand China's cyber security and internet.

As the director general of the cyber security coordination bureau of the CAC, I often have extensive and intensive exchanges on cyber issues with foreign government officials, business executives, and experts. Today I would like to take this opportunity to share with you some of the questions and misunderstandings that have frequently come up in recent discussions. I am often asked about the fact that China is currently formulating the cyber security law, and if that means that the Chinese government intends to restrict foreign companies' operations in the Chinese market.

It is true that China is speeding up the formulation of a cyber security law, which is the first comprehensive law regarding cyber security in China. The internet has been developing rapidly in China; within two decades it has grown from nothing to 700 million data links and four million websites. The internet is becoming an indispensable component in peoples' lives and work, and the Chinese economy and society have come to highly rely on the internet. Therefore, we need to have a constitutional law concerning cyber space, so as to safeguard the security and interests of the state, enterprises, and individuals in cyber space, and to identify their respective roles and responsibilities. Formulating a comprehensive cyber security law is quite a necessity. Personally, I hope such a law can be formulated as soon as possible.

The cyber security law is beyond the work scope of my bureau, but I can assure you that formulating the cyber security law, including the related policies and standards, will allow for foreign technologies and products. As a matter of fact, China's rapid development in the past several decades does not only extend the possibilities by our opening up policy. China's opening up has not only benefited 1.3 billion Chinese people, but has also made a great contribution to the global economy growth. President Xi Jinping had suggested on many occasions that opening up is China's best state policy, and that China never closes its doors – it opens the door to the outside world.

I can give you an example regarding our opening up policy in China. The National Cyber Security Standardization Technological committee is in charge of the national cyber security standardization work. The committee has eighty-one board members, four of which come from foreign companies, like Microsoft, IBM and so on. Recently, some European companies have expressed to me their interest to become

board members of this committee. I can only say to them, "welcome, but you will have to wait until the next elections of the committee".

China's vision of cyber security is having an open environment, and promoting more technical investment and innovation is the best way to address the cyber security issues. Therefore, China welcomes Israeli enterprises and foreign companies, and invites them to invest and do business there. Some foreign entrepreneurs are quite frank with me, and they ask me: "although the Chinese government has promised to maintain the opening up policy, we are encountering more and more difficulties in China and our market share is declining. Why is that?" I believe that the difficulties those enterprises fear do exist, but unfortunately I do not have any magical answer that can make sure the situation only improves and brings more profits, otherwise I would have quit my job and started companies myself.

The Chinese market today is different from what it was only a decade ago. Back then, China's IT infrastructure was in its infancy, and our domestic market was basically dominated by foreign companies. The users had no choice but to accept whatever products the foreign companies offered. Foreign companies in china had few competitors at that time. However, today China has many successful IT companies like Huawei, Alibaba, Tencent and Baidu, and all the while more and more foreign companies are trying to get into the Chinese market. Competition is unavoidable, and may become even more intense.

In addition, users learn more and more about security, privacy, and trust. It becomes increasingly difficult for companies to win the market with their users. It is out of such concerns that China emphasized the requirement of being Secure and Controllable. This doesn't mean we exclude foreign technologies, and it does not protect them either. Neither does it mean that everything must be made in China, or that we would require anyone to disclose source code. Secure and Controllable has many other requirements: the first is to make sure that the user can independently make decisions on user data. Without user consent, no organization should collect, use, modify or transfer users' data. The second is that no organization allows access to changing or taking over user systems without user consent or against user will. The third is that no organization exploits users' dependence on products or services for unjustified reasons, by delaying users' access to the products or services, or threatening to suspend technical support.

Secure and Controllable by no means intends to impose nationality-based restrictions. Technologies and projects, no matter whether they are foreign or domestic, should all be Secure and Controllable. This is a prerequisite to protecting users, and increase their confidence in products and enterprises, and the companies will benefit greatly from it.

The best way to know China is to visit China yourself. Hereby, I would like to extend an invitation to all of you – grow with China together, prosper with China together.

1ST SESSION: CYBER FAST FORWARD

MICHAL BRAVERMAN-BLUMENSTYK, GENERAL MANAGER, AZURE CYBERSECURITY, MICROSOFT

Today I would like talk about cyber security and cyber crime going forward, starting what organizations are currently facing. In the recent past, only ten years ago, it was sufficient to provide protection against known attacks and known signatures, but this is not enough anymore. Even if we defend against known patterns, it is not enough to defend the organization against Advanced Persistent Threats. Such threats are currently residing in organization for more than 200 days before they are detected, if they are detected at all.

Cyber crime is becoming much more sophisticated than before, as an ecosystem and as an industry. We have people that specialize in writing code; we have data specialists whose expertise is to create the merchandising ecosystem; we have people in the cyber crime industry who specialize in creating infrastructure, etc. With this level of sophistication of attacks, and especially when facing an Advanced Persistent Threat, we in the security industry face a situation where nothing is known anymore. We don't have the privilege of learning from the last war, we have to find the *next* war, and therefore we have to protect against threats that are both known and unknown to us, which makes it very difficult.

The security industry is fighting back, and many advances have been made over the last few years. However, the industry is still mostly in its comfort zone. Of all investments in the security industry, 80% are

still in protecting against known attacks and defending the perimeters. In addition, even the best products in their area, which use the most advanced technology – like big data, and machine learning – all of those products are still defending a part of the organization, their silo. What we get is silo products that are doing an amazing job in protecting the end-point. Other silo products are doing an amazing job in protecting the network, the identity, etc. The problem is that many of these products are not integrated, so many time the security operator whose charter is to protect the organization, does not have the full picture. Those gaps between the best-of-breed silo products are utilized by the criminals in order to penetrate the organization, and to create the damage within that gaps that are created by this lack of integration between the various silo products.

Another problem that we are facing with the current security solutions is too much data. Imagine the poor security operator sitting in his post, getting thousands and maybe hundreds of thousands of alerts per day, all of them are at the highest priority. How can you handle all that? Too much data is almost as bad as no data at all. Yes, big data is very important, but our job in the security industry is to make sure that we turn this huge amount of data into very small and precise and concise information, which is actionable, and can be used by the security operator to protect the organization efficiently. We do that by utilizing Big Data techniques.

The next important thing, in light of all the challenges organizations are facing, is that not all assets were created equal. It is impossible to defend everything in your organization, and you have to understand, as the enterprise, what are your crown jewels, and make sure that they are protected. It is very important to protect your organization from the business aspect of the threat, not necessarily from the IT aspect of the threat. For example, there might be two servers, one is holding the marketing collateral, and the second is holding the point of sale or something else that is crucial to your business success. If a malware is attacking those two servers, one of the problems can cause the business to collapse, while the other one might cause some discomfort. It is very important to look at the business aspect of an impact when protecting the organization.

Cyber crime causes more than $2B damages per year, which is much less than the good guys make, so looking at the numbers, it is easy to

see who is winning. What do we have to do in the security industry in order to be more effective, and to provide effective protection against cyber crime and cyber terrorism? First of all, we have to be proactive, not just reactive. This means that we have to employ very smart intelligence, and think ahead. This is much playing chess – you always have to identify what your opponent is planning in order to make sure that you provide effective defense.

However, thinking ahead is not enough. Our systems cannot be siloed, we have to make sure that they are integrated, that information from the end point, from the network, from the identity, and so on, is all connected – and not simply connected and dumped at you, but intelligently connected, to provide the essence of what happened, and of what you really have to protect yourself from. Of course, the protection has to be multi-dimensional, too. Keep in mind that this is war, and like in any war, it is not to fight it alone. We need to create coalitions and collaboration between different parts of the security industry, even between competitors. This is very important in order to win that war, because it is not a war that can be won by a single security vendor or by one cyber crime bureau alone; it has to be a collaboration, a coalition, and only that way we will be able to succeed. I hope that industry leaders in the cyber security industry will get together to see how we can cope with and win all those challenges, posed to us by very innovative cyber criminals.

OMAR ABBOSH, CHIEF STRATEGY OFFICER, ACCENTURE

As part of our work in Accenture, we create simulations of real-world cyber crimes. It turns out that these real-life simulations of adversaries really do work in our clients' boardrooms, and get the board of director's attention to the security topic, and elevate it at a strategic level, only without the nasty real-world consequences. The French cultural theorist Paul Verilio said that whenever a new technology emerges, its negative side is also revealed, at the same time as the technical progress. In my opinion, this is a rather sad viewpoint of the world, but unfortunately it is a correct one. The very technologies that empower us to innovate, particularly in the digital and the cloud arenas, are exactly the technologies that introduce the new vulnerabilities that the attackers use against us.

We at Accenture believe that it is our job to understand these new innovations, those subtle technologies, and the vulnerabilities that exist within them, put them in a business language, and bring the result to the board of directors, to make it a strategic priority and not simply a compliance objective. We see that this is indeed a trend in progress, because our job is to help create visibility for the future course of the ship, and to make sure that this kind of thing doesn't happen on our watch.

Accenture is quite a big company, with 375,000 people; the net revenue of the company is over $30B. We are about $70B of market capitalization on the New York Stock Exchange, we have offices in more than 50 countries worldwide, we serve over 40 industries, and we organize ourselves in five markets: strategy, consulting, digital, technology, and operations. Here I would like to discuss the way we think about the security topic, as well as some moves that we are implementing specifically in Israel.

When we think about our business, we believe our mission is to bring innovations of all kinds into the enterprise to help companies unlock value. Today a major part of the innovation revolves around the digital world, and, of course, digital and cloud create tremendous opportunities, but at the same time brings new vulnerabilities, and we owe it to our clients to make sure we help them manage and mitigate those. With almost 400,000 people working in the boardroom, with our red team, and in the core operation across many industries, we have some perspectives that may be relevant and useful for cyber professionals. In my role, I am outstandingly lucky in that I get to see all the innovations of Accenture working with our clients across every industry, to take a perspective, and ask "what does that mean for us?" as we think about the security topic.

People and organizations all over the world are spending huge amounts of money on security, about $84B, making it a massive market for companies providing products and services in the security space. It is a tremendous growth opportunity, and all the forecasts indicate that it would continue to grow massively over the next few years. The funds are being spent in big corporations and all the way down to start-ups; the VC industry is booming, and in the past few years there has been a major spike around VC investment in the start-up community.

When you ask clients what they spend their money on, you can see sky rocketing predictions of investments in threat intel and other areas that they want to focus on. From the point of view of a service provider or a product vendor, that is great, but the problem is that this method and way of thinking isn't really working. The assaults continue to increase, both in frequency and in severity, and so the risks multiply. Recently we released a research with HfS, which found that 80% of enterprises find that corporate insiders, i.e. employees, have engaged in data theft, meaning that people who work for companies also add to the security problem.

Most of the more public attacks, like Target attack, have been using relatively old school technology – phishing type approaches, stealing credentials. Some of the more recent attacks we see are actually much more horrible: the power grid attack in the Ukraine, which took 80,000 people off the grid for a long period of time, and frankly could have been much worse; the Bangladesh attack that stole $100B and compromised some of the payment and SWIFT systems; and the American super conductor's loss of Intellectual Property, which cost 600 jobs and $1B of profitability. Those are very serious issues, and, of course, in response to that, many companies are working to tackle the issue. However, the risk is very asymmetric.

When I think about Accenture, with nearly 400,000 people, we have a lot of end-points to protect, and it takes just one person to make a bad mistake. Therefore, the most stressed out person in Accenture is not the CEO or the CFO, but the CISO; it is a very tough job that he has to deal with. This asymmetry of the risk, plus the fact that the cost of attacks is rapidly declining, means that any company and any individual, any one of us, is open to attack. There was a time when people thought you had to be rich and famous to be attacked, but that is just not the case now, when everything is mechanized and very cheap.

What is the world doing to address this issue? From our perspective, we see companies working in two primary ways: the first is to buy advice around the general GRC space – Governance, Risk, and Compliance advisory services – to tackle the problem, to think about how they organize policies and processes. The other aspect is massive proliferation of point-solution technologies that address specific issues, which at one level solve problems for the CIO, and at another level, because of the fragmented heterogeneous landscape, create

new vulnerabilities and new problems – a new headache. Those two approaches in combination don't really tackle the issue that we are dealing with.

In our day-to-day work with clients, we work with most of the Fortune 100 companies, the world's biggest enterprises. Our red teams test them in terms of what they have in place, and some of them are the most sophisticated companies with some of the highest expenditure, and we have never yet failed to take control of a target system landscape. The vulnerabilities are there, and they arise from all sorts of issues – sometimes the simplest ones, like an alert that is lost in a fog of false alarms. The operator sends a message and opens a ticket, but nothing happens in the system, and those are the issues that big enterprises are dealing with every day. There is no silver bullet.

We are playing catch-up, asking ourselves what we need to do, I think it is such an important topic is not simply the cost and expense on security systems and products, but the massive opportunity cost of not conducting nimble agile business in a digital world. Companies spend so much time protecting themselves, they take their eyes off the ball when it comes to innovating and growing, which is actually the real risk to our economy. The attackers are sophisticated, nimble and nasty, they share their IP on the dark web, they buy and they sell the IP, and so the malicious methods can move very quickly. But how about us, the people on the good side? The answer, unfortunately, is that we are remarkably fragmented and siloed. Thus, the greatest challenge in competitive industries, with laws around data and regulation, is how to collaborate much more swiftly than we do today.

The bottom line is that the current model, of spending more and watching the attacks increase, is not a great option, and we have to find a different way to go. It is all about harnessing a power of collective ingenuity, getting the power out of the whole ecosystem of people who are acting in a positive interest. No one company has the monopoly on innovation. We are currently being out-innovated by people who share their innovations, and we need to share our innovations from a wide ecosystem.

How do you get the power of the ecosystem and use it against our adversaries? We propose a more collaborative approach. I genuinely believe that using some of the things I am about to mention will help

make the bar much harder to climb for the attackers, make it much more expensive for them to attack us, and certainly eliminate some of the easier hacking beginners, and perhaps affect criminal gangs and terrorist agencies – although, of course, with nation states who are bent on this course of action, a much more sustained approach will be required, and no one thing is going to solve that.

There are three pillars to this collective ingenuity. The first one is taking an industry lens on the world as you think about security. A company called Ponemon did a survey last year, and found that less than 25% of companies share threat intelligence in their own industry, and I think it is completely mad. If industries could collaborate more to understand the threats that are pervasive in their sectors, they would do a much better job about responding and reacting.

We also see security providers providing solutions that are generic and consistent across industries; it also doesn't really make sense, because you have to understand the nature of every industry, understand the attacks on each industry, understand the nature of the attackers who are interested in that industry, and what are they really after. Therefore, this point about applying an industry lens is crucial, and in Accenture we think about what it means if you are an oil and gas company running a refinery or an offshore rig, if you are running an autonomous vehicle and a connected car system, if you are trying to protect the molecules of a life sciences' company, or if you are trying to protect yourself against bank fraud. Those issues are all very different, so it makes sense to understand the different adversaries, the different attack surface, the different systems that are employed, the different controls that are in place. Only when you have the full visibility of the attack landscape in that sector, you can really put together the appropriate and strongest mitigation and defense approaches to develop the most resilient enterprise; and for that reason, I believe that sharing information within industries and sectors is very important.

The second area I would like to talk about is developing a healthier business immune system. It turns out that of course technology is indeed a crucial piece of how to do this, and we are seeing an emergence of a range of new technologies that at Accenture we think are very interesting and very important. As you know, the perimeter-based approach is not doing the job, and similarly, most of the technologies employed today are monitoring and reactive-oriented. Our thinking

is that actually we need to automate as much as possible of the monitoring and the reaction, to free our investment capacity, to move it towards more proactive techniques.

The problem is, of course, that all this technology is expensive, and so how do you prioritize? The role of the senior executive is to think about the investment prioritization. What we are seeing is the emergence of a range of platforms that are very supportive of the automation of some of the remediation and monitoring parts of the job here. The platforms are using extreme data science and very advanced visualization techniques. For example, if you have a platform monitoring intelligence feeds for multiple companies in a sector, using AI and machine learning it can spot anomalies faster, you can figure out which is the nastiest, and then you can put out a warning across the companies and the ecosystem to create more of a threat intelligence ecosystem than we have had before. We are actually seeing the emergence of techniques that move beyond looking at what happened yesterday, find out what is wrong and then copy that, and moving to find never seen before vulnerabilities, as well as the emergence of cyber hunting techniques, where within your own virtual network you can point, shoot, and kill the adversary that's inside your domain.

The combination of those sorts of techniques can be extremely powerful. Similarly, with advanced visualization, one of the dirty secrets of the security industry is that the typical average dwell time of a hacker inside our environment is 150 days, which gives them enormous time to wreak whatever havoc they want to. We have to be able to move faster, and currently, in Accenture labs, we have a system that is tracking 2 million other systems in real-time with actionable alerts, using advanced visualization with super-clever clustering techniques and security analytics, actually mainly on open-source technology like Spark, which allows us to move much more quickly than most of the readily available commercial systems that typically track about 10,000 systems at a time. This scalable visualization, with the cyber hunting I mentioned, can give companies a real jump on the attackers, and make their job that much harder and that much more expensive.

We believe a holistic approach to security is essential, and so we bring together a very wide range of security techniques and technologies into our cyber fusion centers. We have these now In Washington DC, in Bangalore, in Prague, and now also in Israel. Our cyber fusion centers

are supporting our clients and sniffing out their potential vulnerabilities, and helping them respond in pace. It's in those places that we operate our own cyber defense and cyber intelligence platforms, using the sorts of technologies I just mentioned, where we bring together our own ecosystem of partners. Also, to build the hardened defenses, the immune system, you have to understand that an attacker is not a one or zero, they are not a noise on the wire, there is always a human behind the adversary; and understanding their psychology, understanding proactively what are they really after, in order to create the right defenses, is crucial. This is why we bought a company called FusionX, which specializes in simulations, and actually taking on the control of the clients' ecosystem.

We believe that you have to assume the attacker is inside the perimeter. Therefore, a full end-to-end approach is the only way that works, and we are putting our money where our mouth is. I am very happy to announce that we are extending that logic – we made an acquisition of Maglan here in Israel, bringing into the Accenture family another group of super-experts in this space.

The third part of our strategy is about driving innovation deliberately through the ecosystem. We believe that every company needs to find its own ecosystem of where your innovation happens in the security space, and you bring this to defend yourself, so you can take a much more collaborative but also aggressive approach towards the attackers. Accenture plays a role as an interlocutor between the innovation that is happening in the technology and industry ecosystems, and bringing that to our clients, and we look forwards to doing much more of that. And what is a better place to do so than in Tel Aviv with extremely smart and brilliant minds in the cyber community, more than 300 companies, start-ups in the cyber space, which means that Israel is number two only to the USA in terms of the scale of the industry.

And indeed, we are opening a cyber lab in Israel, as part of the network of Accenture labs, where we will do our security R&D. The cyber lab will focus on the latest in threat intel, active defense, passive detection techniques, IR, as well as state of the art forensics, malicious software, analyses and IoT security, all with the idea of being applied within the near term at our clients. As you can hopefully tell from what I am saying here, we don't think that our business is just about methodology and advisory and implementing technology, we think it

is about harnessing the full power of an ecosystem of innovation and bringing that to our clients.

As a public officer of a listed company I understand exactly the issues around sharing data sharing information, but hopefully you can see that we really believe that this business of using the network the ecosystem to drive the innovation is exactly the way to tackle the cyber crime and the sea of cyber issues that we see in front of us today. We believe that if we can go past the day-to-day of worrying about protecting ourselves from security, it gets us back in our day job of innovation and growth, and that is exactly what this is all about.

We are constantly looking to connect with the start-up ecosystem, companies, academics, and all the people who are deep in this space, to figure out what is the right ecosystem for your business and how to get into a more proactive start to tackle this – how do we harness the power of the collective ingenuity to innovate and build more resilient businesses together. It seems to me that the attackers' motives are relatively well-known, and we need to draw more power from the ecosystem to fight back, and as security leaders in the space, we owe it to the public and the business world to do that. We are trying to help the good guys become more of a force to be reckoned with.

GIL SHWED, FOUNDER AND CEO, CHECK POINT SOFTWARE TECHNOLOGIES

Many people ask me, "how do you think the industry needs to change and is going to change?" In my opinion, the major focus of the industry should shift from detecting attacks to preventing them. One of the greatest cyber security challenges is the growing threats. In the last year alone, there was an increase of almost a 40% in cyber security attacks. Major discussions are being held in every boardroom, with 80% of board members indicating that cyber security has been discussed in every board meeting, and two thirds of them are not confident that they have the right strategy. Those two thirds are the ones that know what is happening in the world. The other third, which is confident that everything is working fine, are the people who don't know what is going on.

Why does this happen? And why do we invest all that time and funds, and yet at the same time we have such big challenges – and especially

when we draw the analogy between our real-world, or the physical world, to cyber space? Fighting against cyber space is very different than real-world wars. For example, I recently visited a bank's security operation center, and they showed me some interesting statistics about bank robbing and conventional crimes against the banks. Such crimes, which we have been fighting for hundreds of years, happen 2-3 times a year. What is the potential damage? The bank doesn't keep more than $5K accessible in every branch, so the potential damage is about $10K a year. In contrast, if we look at the cyber security operation center of that same bank, they see about 20-30 per hour, and the potential damage is over $50M, and this is only from attacks they were able to detect.

There are many differences between conventional attacks and cyber attacks. In the conventional attack we have very clear boundaries, a very clear territory, we know who can attack our country, we know who is around our house; we know the limitations there. In cyber space, the attacks can come from anywhere on the globe, we don't necessarily know who is attacking us, and that makes it much more difficult to collect intelligence and to stop the attackers.

The same thing applies when you compare weapons that people use in conventional crime or even conventional warfare. The weapons there are quite basic: gun, knife, even a baseball bat can be used as a damaging tool. If you look at the cyber attacker, any kid and any criminal can have access to the most devastating tools. You can see, for example, that the Locky toolkit and the Stuxnet virus were invented by cyber super-powers, and suddenly, in a day, they became tools available for any attacker or any kid on the block. If we try to look at that same analogy, in cyber attacks, the attacks can come from anywhere, they can target anyone; these are automatic tools, which scan the network. They can come at any time, and they use the most damaging tools – not just the basic tools that we are trying to fight on a day-to-day basis – and that makes all of us very vulnerable.

So how can we stay protected? What do we have to do differently? In conventional protection, we rely mainly on detection and alerting, we have a security camera, and we think that if the attacker will be seen they won't attack us. We have an alarm system, and again, we think that if the sound will go on, the attacker will go away. But what happens if they don't? We think that we will catch them and punish

them, or, in the case of nation-wide security, we will retaliate. Our key weapon is basically the deterrence. The attackers will be afraid, because there are consequences to something that they will do to us.

Now, let's look at cyber protection, and see if all of these principles apply here as well. Detection and alert: it is quite hard to detect many of the attacks, they are very evasive. Can we punish them? The alarm can go on, we can have alerts that somebody is trying to break into our system; the attacker who is inside the system doesn't care – they sit in a completely different place in the world, they use a server in a different continent, and they don't care that you see them doing what they are doing. Can we fight back? In most attacks, there is really nobody to fight or to punish, and you can see that the number of cyber criminals that are being caught is very, very small, definitely compared to conventional crime. When we think about deterrence, there is really nobody we can discourage, and it is very difficult.

Our technological system and our legal system are not built to deal with these kinds of attacks. So, what can we do? We need to think differently about cyber attacks. We cannot rely on the conventional thinking and on the traditional tactics, and we cannot rely on the fact that if we detect the attack we will be able to end it. It may sound obvious, but when we conducted a survey in a recent cyber security conference, and we saw the companies that presented new technologies, almost 80% of those new technologies focused solely on detecting attacks – and again detection alone is not enough, we need to look at a different approach, and that approach cannot be on the nation level.

Many people invest hundreds of millions of dollars in building security operation centers and cyber rooms, which collect intelligence and detect attacks, but in the end, there is very little we can do with that information. We need a different approach, arguing that we can prevent the attacks, and so we need to focus on prevention. That is our mission, we need to help and we need to think one step ahead about how to prevent the attacks.

So how do we prevent an attack? What are the main principles? First, we have to focus on blocking; second, we need to defend ourselves with the most advanced technologies, because we need to block not only yesterday's attack, but tomorrow's as well. However, if we don't block the attacks from last year and from fifteen years ago, they will

also come back; so we still need to block all types of attack, old and new, and mainly we need to focus on tools that will block tomorrow's threats. Finally, we need to look not only at the conventional places where we used to stop attacks, but at every frontier, from our mobile to the Cloud. It is not enough to look and say that we have one solution, ten solutions, twenty solutions, and a typical enterprise today may have more than two dozen different solutions for security. We need to look at security as a single system with one strategy, consolidating all the elements into one system and one architecture, and that will help us to block attacks before they happen.

In Check Point we look at two key areas. The first is what we call "zero-day attacks", attacks that are yet unknown and we need to prevent them. For this we have a technology called SandBlast. This is one key element that blocks the new attacks that we still haven't seen, and does that in real-time.

The second area is mobile devices, which is the real new backdoor into all of our lives, our enterprises, and our countries. All the information that we see and hear, information that surrounds us, is going through these devices, whether we know it or not. These devices hear us all the time, they see us all the time, and they broadcast all the information that we see, all the time, through the public network, so we don't have any control over them. For this reason, protecting the new mobile forefront is a very critical element, and yet, not many people have a mobile security app or other mechanism on their mobile phones. This is very uncommon even among security experts, and when it comes to the general population I believe less than one percent of people use anything to protect their mobile devices.

Protecting mobile devices is not simple. If we look at the SandBlast technology, for example, there are over 27 technologies that prevent types of attacks in different methods in this simple buzzword that I use. SandBlast is designed to work against zero-day attacks, and every month we add new technologies that can fight new types of attacks and new generic types of potential attacks.

We need to take all the information and everything we have seen, and collaborate. We operate a network called ThreatCloud, through which our customers inform us about the attacks that they have seen, and in real-time we translate them into protection. That way, if one

customer conducts the security analysis automatically and sees a new type of attack, this attack will immediately be blocked by all the other customers and by all the other networks. There are more than 50K networks on this ThreatCloud network, already operating in real-time – not tomorrow, not in five days – because the damage of the attack starts this second. To give you some insights on the system: every day we add to the network over 100K malicious domains or URLs; every day we add to the ThreatCloud network 600 file characteristics, different file types that can be damaging. This is a huge amount of information.

Last but not least, we need to look at every frontier. If in the past we focused on our personal computer, which is the end-point, today we see networks with 400K such end-points, which is a big network that needs to be protected. We at Check Point focus on protecting the network and everything that is going through the network gateway. That isn't enough in the modern world, that was yesterday – it is still very important today, but we also need to protect the Cloud, and look at the virtualized data center, some of it may be on our premises while some of it may be outside our premises. We need to look at the mobile area, which I already mentioned, and I believe it to be the real backdoor to the enterprise these days. But this is only today; if we look at the future, we need to look at the Internet of Things. Any device that we carry can be a backdoor to our network.

We need to look at the national security level again, not simply collecting information or just building security operation centers that give us intelligence, with no army to stop the attack, no army to fight. We also have to look at our critical infrastructure. This is not something that we will need in the future, these attacks already happen, and we need to build the systems for that future. We are moving from network and end-point to a much broader landscape and a much broader universe that we have to defend.

To summarize, in the past we used strategies that were mainly reactive; we have seen a new type of attack, and used many detection products. Now we need to move to a strategy that is proactive, holistic, one that is focused not on detection, but on prevention. If in the past we looked at two major vectors of attack – network and end-point – today we need to look at a much more holistic space – network, end-point, mobile data center, and the Cloud – and if in the past our architecture was point-solution, with multiple consoles and complicated management,

we need to look at one consolidated system, with a single strategy and single management. We encourage everyone to think about this challenge that we face, how to build one consolidated system with single management, which takes security one step ahead, to be ready for the future.

CALEB BARLOW, VICE PRESIDENT, IBM SECURITY

There is a paradigm shift we see today in cyber crime, which is now one of the world's largest illegal economies – $445B in annual illegal profits, centered around more than one billion pieces of personal information. One important thing to remember about cyber crime is that 80% of what we are dealing with is not "bored teenagers" or even nation state actors; its simple organized crime. That has been the norm in this business for years, but there is a paradigm shift happening right now in fraud, and it stems from the fact that you don't need to be technically sophisticated to launch a cyber attack anymore. Eight or Ten years ago you needed to be an expert in technologies like Python, HTML and Javascript in order to launch an attack. However, today you know you don't necessarily need to know about networks or even have familiarity with browsers and switches. In fact, you don't really even need knowledge about computer security at all. What you do need is to be an entrepreneur, and have a little bit of money, and you can invest your way through an attack. Because, like everything else, cyber attacks have gone to the Cloud, and became Software as a Service.

Before we can go into that in more detail, we need to establish some definitions. The first is what we call the "clear net". This is where you and I all operate in our day-to-day. You can think about it as all the websites that are accessible through a google search. Now the IBM X-Force Threat Intelligence team tracks 25 billion websites, URL's and images on the clear net every day, looking for fraudulent activity. It is not exactly the easiest place for the bad guys to hang out. But then we move to the deep web. These are sites that are protected behind a firewall, and protected behind a user ID and a password. In fact, 85% of the information on the internet exists somewhere deeper than the clear web. This is a better place for the bad guys to hang out, but still, if law enforcement manages to get access, they can still track down the IP address, which leads them to the server, which leads them to

the hosting environment, which eventually leads them to the bad guy. The best environment for a bad guy is the dark net, which is an area of the internet where you can operate anonymously; where you can buy, sell and trade goods and services, including fraud, data, drugs and anything that might be illegal. In fact, you can even move money without anyone knowing who you are. These days, it is extremely easy to enter the dark web and build an attack. Gone are the days of technical hacking, enter the days of the lazy man's hack, where all you need to do is a search on google and download a specialized software that will get you access to the criminal underground that is the dark web. When it comes to fraud, one of the first things that the dark web allows you to do is buy and sell people's sensitive personal information; their identities. In fact, you can even build a false identity, which allows you to commit fraud. Marketplaces like this offer you the chance to search and browse different dates of birth and social security numbers, that have all been parts of previous world-wide hacks. Medical records, it turns out, are the highest profile target for hackers right now, as they yield the highest margin in the dark web marketplaces. This is for a good reason – they have the most data on you. You can also buy false passports and other critical information to get out of the country, perform a scam, and even send bills to unknown addresses. And if passports aren't enough, you can also create a driver's license and credit card; an entire false identity. There is no limit to what can be transacted. There is a vast amount of data available on the dark web, and it's all up for grabs. And the scariest part is that it could be yours. Beyond the data, there are also advanced attacks that exist today in the dark web; RATs, exploit kits, malware, fishing, and more.

I already mentioned this is a $455B industry, and this is where it comes from. Suppose you want to launch an attack. Just like a general contractor in charge of a building, you can outsource to various subcontractors. The general contractor doesn't do the electrical and the plumbing themselves. You find the right people with the right tools. You can view hackers' résumés and reviews to see if they have the skills that you desire. You can build trust in an untrusted environment with these reviews, build teams, and collaborate to make sure you have the right resources to pull off that attack and find the hack that is right for you. You can even buy or rent these attacks. For example, you can purchase a Ransomware as a service, and take part in the upside. Alternatively, if you want to build a hack yourself, you can just

buy and download the tool. And it isn't just fraud, either. The dark web is a marketplace for anything illegal, and it is all anonymous; the buyer, the seller and the transactions are all completely protected.

Looking into how many people are actually using the dark web; the answer is millions. We do have to remember that the dark web actually has some legitimate purposes as well. It is being used by political dissidents, reporters collaborating with sources, and the thousands of people that sit in countries around the world where the internet is censored. But we have got to stop admiring the problem; we have got to come up with a solution, and I propose that part of the way we do that is to become strategically proactive in what we do.

The problem is actually very similar to a pandemic, and we need a similar response across governments, private industry, and cyber security companies. We need things like data protection, application protection, network security vulnerability assessments, and the list goes on. In order to assemble the right tools and solutions to do that, we need a framework. First, we need to organize this over a few key deliverables, and we can use the IBM secure framework as a basis. It is not very different from NIST's, or COBIT's, but it allows us to look at each of these elements of security and ensure we have both breadth and depth. This isn't just about building the castle wall; we also need the mote, we need the archers on the wall, we need the sentries out in the village, and all of this has to come together and bring back intelligence and information. All this flows up into a security intelligence layer, which gives us the analytics and the ability to look at what's going on across the spectrum of security.

We established IBM Security four years ago as a start-up in Israel, and in those years we assembled 7,500 security professionals, a thousand of which were added in the last year alone, and have reached a $2B annual revenue. On top of that, we just completed our 20th start-up acquisition in the security space, making us not only the fastest growing, but also the largest enterprise security company in the industry. Israel is a very strategic location for us; IBM has acquired 14 companies in Israel, and after the USA, Israel is the second largest location on the globe, with 500 security experts. Companies like Guardium, AppScan and Trusteer, along with the Beer Sheva lab at the Cyber Center of Excellence, are all key parts to our strategy. Israel is our world-wide center of research for banking fraud: at Trustier we are servicing

more than 100 of the largest banks in the world, keeping the money of millions of customers safe, and our SIEM solution, QRadar, was selected by the National Cyber Bureau to serve the government CERT, and to be a national SOC for the government.

We, at IBM Security, are working on several innovations in this area. Over the course of time, what we think of as the "traditional" perimeter has become blurry; more and more data is moved to the cloud and to mobile, and we need to protect that data. One of the tools we use to do that is something called Cloud Security Enforcer; Gone are the days where we could tell people they can't use the cloud, because the reality is that end-users are going to do it anyway. This tool provides them with better and more secure ways to do it: by guiding them to solutions that are sanctioned by your enterprise, by allowing them to still use the cloud but do it with the enterprise credentials, so that when they leave the company, or when their device or account is compromised, you still have control over the data.

The second thing to discuss is X-Force Exchange. At IBM we firmly believe in the importance of democratizing threat intelligence data. We do not charge for our threat intelligence data, and we have published everything we know on a social network for threat researchers called the X-Force Exchange. Moreover, all of IBM's X-Force threat research is published there on a near real-time basis. We are very committed to doing this, as we believe we have to change the economics for the bad guys, and the single best way to do this is to make their attacks only viable for minutes or hours. If any one of us detects the attacks and shares it with everyone in the room, then we all become inoculated to that new virus or malware. For the bad guys, this is a big problem, because we are not up against bored teenagers; We are up against highly organized gangs of 20-30 people, that have invested tens of thousands or hundreds of thousands of dollars in developing that new attack. If it is only viable for minutes, then that attack loses all validity. But we believe it has got to be about more than just enabling threat sharing; we need to open up the engine behind it. If you are a security start-up, you can actually integrate your solution with QRadar, allowing us to extend that ecosystem beyond just the innovation that we produce at IBM.

A part of what we have to recognize, is that most of the information we deal with as security professionals is by and large structured data;

it is the tip of the iceberg; it is events and logs and network activity. But 85% of the security information in the world is designed to be consumable by human beings: research documents, publications, transcripts of conferences. Today, on average, an organization sees over 200,000 pieces of security events' data per day, spends $1.3M a year chasing down false positives, and wasting nearly 21,000 hours in the process. Coupled with 10,000 security research papers published every year, and more than 60,000 security blog posts each month, and you quickly realize the problem.

IBM's "game changer" is to apply cognitive solutions to this problem. We do that by using IBM Watson, the same tool that we have focused on solving cancer, and addressing the jeopardy grand challenge. Our goal is to start using cognition to break down this barrier, to be able to respond to threats with greater confidence at scale and at speed. To give an idea of how this works, and how we start to get underneath that unstructured data, I will use an analogy of an ambulance responding to the scene of a head injury. In cases like this, interestingly enough, a diabetic emergency, a head injury or someone who is just intoxicated, all show the same signs and symptoms. How does the responding paramedic know what to do? They look at the structured data, such as the patient's pulse, respiration, oxygen level, and blood pressure, but they also look at unstructured data: this was a car accident, the patient hit and cracked the windshield, etc. They also think back to the conference proceedings from two weeks earlier, where they learned about head injuries. All of this information comes together, and when they go to the hospital they have an interesting cadence with the physician: "I responded to a 25 years' old victim of a motor vehicle accident. I believe this to be a head injury, as they hit the wind shield, their speech is slurred, and their pupils are not equal or reactive to light". They provided evidence, and they backed that evidence up.

This is exactly what we are doing with Watson, and today we are training Watson to learn just like a human being. We have to ingest up to 10,000 documents every month in order to help Watson manually tag them. Just like a human would learn what is an adjective, what is a verb, and what is a noun, Watson has to learn what is an attack, what is a victim, and what is malware. We are training Watson to take on this challenge, and be able to augment our security researchers. By 2020 there will be around 1 million open cyber security jobs, and we need all

the help we can get. Some of this work is happening in Israel, as IBM is partnered with leading researchers at Ben Gurion University (BGU), working to train Watson. Specifically, we are working on advanced mechanisms for knowledge representation and high-performance engines for answering questions. This work is being coordinated by our cyber security center of excellence on the campus of BGU, which drives many other joint projects with the university as well.

This is a problem we can all solve together, but it means we have to think about new technologies and new ways. We have to work together to bring innovation to the forefront, and most importantly we have got to democratize the data that we deal with every day.

UDI MOKADY, FOUNDER, PRESIDENT AND CEO, CYBERARK

We are in an ever-evolving industry, and CyberArk is very proud to be a market leader, but also a very adaptive company. Today I want to talk about how we changed our mission, and how we appeal to everyone to change yours. Our job, as a global cyber security company, is actually to worry, and that is what we do every day, all the time. Usually, we are here to help customers and partners make sense of what's going on in this very hectic cyber world, where the stakes are very high. But beyond that, I am worried because many customers take a project-siloed approach to security, and when we look at how the attackers are, sophisticated compliance-driven projects are not securing our customers. What we are talking about is that we should stop talking about security projects and start thinking in the concept of programs. Our world is all about protecting the inside of enterprises against credential theft escalation of privileged and full account takeover.

Today, businesses run on IT; every modern business, even a trucking company, is running on IT. What does it mean to lose control of the business? Recently, a hospital in Los Angeles lost control over the digital assets due to ransomware; their e-mails and many of their digital health care records were lost to them. Patients hospitalized there had to be moved to other hospitals, and they eventually paid the ransom, they paid the hijackers in order to get the ransomware out of their systems.

Losing control is what happened at Sony where they had to rebuild their network from scratch, even moving to manual paper-based processes

until they got that in place. And recently, the SWIFT credential theft led to full control of the attackers, as if insiders were operating the network; loss of control over financial transactions based on SWIFT. Last year, the American Office of Personnel Management was hacked, in one of the largest breaches ever – more than 20 millions records of federal employees were stolen; but not just renewable records that maybe you can call and change. You can't change your fingerprint. 5.6 million fingerprint records were stolen. This is what losing control looks like.

Our mission changed over the years. When we started CyberArk, we were happy to please customers who were going for compliance-based projects. It got them the funding, they got rolled out, they had credit from their auditors, the CIO was happy, and everybody moved on. But what we saw is that compliance if far from being security, and the attackers were becoming more sophisticated and started operating more on the inside of the networks, and so we have adapted. We took our privilege account security, and turned it into a platform that takes into account that the attacker is operating from the inside the network, stealing credentials, and moving laterally to take over the enterprise. We adapted it to create a new layer on the inside of the enterprises, and that is the mindset from which we created this platform inside organizations. To do so we had – and this is our goal – to limit the damage that can be caused by an attacker who made it inside and is working like an insider; to prevent and stop lateral movement, because once you infiltrate a network, that is how you steal credentials: you move from laptop to server, and try to work your way up to escalating privileges. To stop that constant movement and credential theft, contain the threat, and avoid the complete network takeover, like in the Sony example, where the passport authority of the organization has been taken over and full control was lost. And so, CyberArk's mission has become to really help our customers build and maintain trust in their IT systems. And to do that, we had to change.

As part of adapting the way we work according to the way the attackers work, we actually changed our R&D to work in an agile development format, and we took it to the extreme. These days, CyberArk is considered one of the best practices in working in agile development; many other vendors come to consult with us on how to make it happen, work interactively with customers to come out with customers quickly and

address their real needs. And we have expanded our offering, from proactive protection and putting controls over aggressively rotating credentials, to also understanding the ability to detect the attacker that already holds on to a credential, or somebody who came on the back of a third party with strong access, so that we can detect it and stop it.

Beyond our organic development, CyberArk went public in 2014, and in 2015, our first year as a public company, we made two acquisitions, both had R&D here in Israel, to expand our offering to the earlier part of the infection, and to expand privilege account security to the end point, so that we can detect and stop the accounts earlier in the attack life cycle, while trying to prevent the end-goal of full control over the network. We have also been collaborating closely with our 2,600 global customers; we have 40 of the Fortune 100, and more than 20% of the global 2,000, very sophisticated customers that are living in this changing landscape, so that we can adapt to how they are adapting and changing their continuous adaption of Cloud assets, and give them a hybrid solution from both their on-premises and Cloud-based assets. Collaborating is also creating alliances. Only a few weeks ago, we announced our global technology program, called the C^3 Alliance, which is very bi-directional. We created a platform where there is a central way to manage privilege credentials.

Privilege credentials are also in security systems. If you are able to capture the administrative console of a security product, you can just open the gate; but this is another thing we made bi-directional with integration, where we can feed alerts. We can also collect alerts, so that our customers can do "one plus one equals three" with the other investments they made, such as other companies' products, e.g., Check Point.

We believe that there is no single silver bullet, and our goal is to make our customers secure by also creating a secure fabric together. Beyond the agile development, another area in our company that evolves rapidly is what we call the CyberArk Labs, which operate in Israel, and have the authority and power to think like the attacker, investigate attacks and solutions by thinking like the attacker.

Imagine an attacker that is already inside the network, in a post-breach scenario. How would an attacker propagate? How would they advance their attack and come up with solutions? We deconstructed

the Ukraine attack to understand how that happened. We looked at the Bangladesh and the SWIFT attacks, and how credential theft happened there. We also investigate, of course, how we can better help our customers and protect them against the effect of ransomware, leveraging our recent acquisitions with solutions from the end-point, and not just limiting the ability to infect of the network, but actually eliminating the ability of the ransomware to get to the encryption of files on the network.

We are also researching areas related to risk based in other systems, and we recently announced and disclosed a weakness that we found in the ability to go after security logs, and not just come with privilege access and delete them, but also tamper with them – even with security logs that have been trusted until now. These are some of the things that CyberArk did to adapt and change, but the mission to change is for all of us. We certainly have to get into this paradigm shift that the attacker is operating from within the network, and then look at the post-breach scenario. For some companies it would be a little eerie to think about it in this manner, but it is the only way to prevail.

We have to out-think, out-clever and out-maneuver these attackers under this paradigm that the attackers are already on the inside. What does it mean? What is the organizational shift that is required for it? For our customers, it means to think in terms of programs and not in terms of siloed projects. Think about it as a long term, continuous work, which has to be done to secure the enterprise. Don't think that compliance is security, the auditor is not the enemy, the auditor is often on your side, and is pointing a little flashlight. The hackers read the regulations too, that is not security. And, of course, push the various vendors to collaborate. Like I always tell my customers, never trust a silver bullet solution, but rather a collaboration approach between vendors. The vendors, on their part, have to acknowledge one thing: there is an immense shortage of staff and security professionals. I am very excited about some of the things that are happening in Israel to change that situation.

Israel has great programs coming out of the army, but also great programs that are currently entering high schools, but this is just the tip of the iceberg. There is a massive shortage of millions of professionals out there for security, so as vendors, we have to help our customers with more automation, more solutions that work better

together, instead of forcing them to be even more behind on the staff shortage. And, of course, we have to better integrate together, in true integrations that have been tested and work on the customer side. This is the main thing that is required from vendors as we change and adapt to the mission.

Israelis tend to be very direct, and some say that it's a part of our advantage. We are very open and transparent with our customers in the approach we take, and even though it's scary to think that the attacker is already inside the network, we can be on a much better trajectory. This is what CyberArk does every day, we have adapted our mission, go adapt yours.

2ND SESSION: SPOTHLIGHT ON CYBER INNOVATION

DR. DORIT DOR, VICE PRESIDENT OF PRODUCTS, CHECK POINT SOFTWARE TECHNOLOGIES

I have been in Checkpoint for twenty years, and that is a great route to look at innovation and how Cyber security evolves along these years. I think one of the things to notice in innovation is that innovation in cyber is a little bit different than in other areas.

What is so special about innovation in cyber? First of all, we are not in control of the situation. There is an adversary out there, who changes the data sets, the attacks, the landscape in which we are being tested; so while we want to create an artificial space in which our ideas and our innovations are showing great results, we have to test them in real life – we have to test them versus the adversary, and the adversary keeps changing constantly. We can't ignore the data set; we can create our own data sets, but this is not the reality. When we will come to POC with customers, they will test our assumptions with their own reality. So, one thing is the attack space and the data sets that are not in our control.

The second thing that is out of our control is the usage and the user. The usage is, for example, that people move to the Cloud, to software-defined networking, to systems of type X; all these things impact the

way we deliver our security, and this is out of our control. People will not change the way they do IT because of the way we want to defend the world, we have to defend the world in the right places for the new and modern IT. Then there are the users. This is an even bigger problem, because the users are completely out of our control, and some would say that they even act against us: if we tell them not to do X they may still do X, either because it is convenient, or because they don't understand the importance of what we are trying to tell them. So users are not acting in favor of us defending them, the usage scenarios are not acting in favor of us defending them, and the data sets and attacks are being forced on us. Now we try to bring technology into the picture.

When talking about innovation, many people will consider the technology part as the actual innovation, and it is indeed a great part of it, but innovation in cyber security is much broader than that. We can't just come up with the technology alone to the innovation; there are areas like the Cloud, promoting innovation, and even challenges in the innovation space, that need to be considered and addressed. These are all tied together in this triangle, and it is very important to understand that when we come to explain our innovation. We can't just ignore the big picture and look at our own technology as a silo. In addition, both vendors and customers have to solve the real problems. Many people say, "okay, here is innovation", and they don't realize that the same statements are heard from hundreds of companies every single day. We all learn to say the right marketing terms; we say many buzz words, and so the customers don't know what to do.

The first action of innovation is to get noticed. Even if you have the greatest innovation, you may be ignored just because nobody knows what it is, unless you figure out a way to get your innovation to the front line, and be understood by a wide variety of people. One way to do that is to be measured. In this industry, we stopped measuring ourselves. Each of us comes with a solution, saying that nobody else has ever solved this, but there are hundreds of people, each with three solutions to things that were so far unsolved. The user is not going to buy a hundred different solutions, they have to measure the things that are most important to them. They would usually do this in a POC: they will create their own data set; their own environment; their own types of favorable attacks, and they will measure your innovation against

the scenario that they built. The judgment of whether or not you are doing a real thing is not just in what you are able to show, solving a real single attack, but in showing it in a real customer POC. Can you convince the customer do to the POC that will show the case? If the customer puts you in the network, will they see any relevant event within the next 30 days so? How would they know that it's worth it for them?

Another element of showing up and solving a real problem is this: if it is a real problem, then it has budget. Is it already in the client's budget? Is it something they already noticed? Is it a niche problem, an isolated problem that the client will have to invent a new budget for?

I will try, very quickly, to review the bigger picture: we need to provide a variety of solutions inside the customer's problem, tying them together, either through partnership, or as a single point of view, and we want it all to be innovative, which in turn comes from understanding the attack surface, from understanding the customer's challenge, and from the freedom to imagine new solutions.

I will give two examples of technologies that you could imagine within the big picture, but each of them is a point technology that comes to solve a problem, and without the bigger picture do not add the required value. One example is about attacks not originating in malware. The most common way to attack without using a malware is to steal your credentials, which is not difficult to do: you could trick the user into giving them by behaving as someone else, or you could find a place where they already use these credentials, and assume that they have re-used them somewhere else. These are relatively good tricks to steal the end-user credentials, because from the moment that I sent out my tricks and asked you to put your credential in something, I have a few hours until I am blocked; it takes seconds, or minutes at the most, for the user to read the email and give out their credentials, and hours before anyone notices and the system shuts down the account. This shows us that the challenge has to be linked to the data, online, in real-time and to defend it in real life. And while it sounds like consumer problem, it is actually an enterprise problem; people have many passwords and they don't remember all of them, so they either write them on a board, stick them somewhere, or they use their own beloved credentials again and again. As a system administrator, you may think your users use special credentials in the enterprise. but

they actually re-use the credentials they use in their consumer life. The other side of this is websites. If nobody could imitate websites, there wouldn't be a problem, but we see sites being copied all the time, and we see people using this to steal credentials. This is a real problem, and it is one of hundreds of similar problems that you have to solve in order to make your users secure. No other problem-solving – malware or any other parts of the problems discussed so far – will solve this problem. This is a problem that needs a direct solution and a direct innovation in order to solve it. This is a problem that needs something that will be a zero-day solution, immediate. You have a very short window before the site gets closed and disappears; before you understand that somebody stole your users' credentials; that this is an imitation site, used to understand if credentials are re-used.

Another example is understanding the attacks themselves. We looked at a single problem, this time understanding forensic information. There are tons of information and events, you could sit down many people to go over events and analyze them, and they need the right education. For that we formed a team of top malware analysts, and we asked them: "can you create a program that will do the analysis that you will do?" A few years later, with multiple patents we were able to take a problem with many events inside, examine all the data that gets collected from these events, and create a coherent picture from all of that, something that will make direct sense, and put it into an application. What makes sense is to understand the exact flow of attacks; what drove the event itself? What DLL downloaded the events? and so on.

These are very good point solutions, they bring a lot of innovation, they give us the freedom to imagine within a space of the problem. But the challenge for our panel will be: can we imagine a place where threats are being blocked early on, before they do damage? And are we solving the real challenge or just finding point solutions? I think this is the challenge for all of us. We all enjoy bringing technology for the point parts, but we have to solve the whole picture of things.

BHARAT SHAH, CORPORATE VICE PRESIDENT, MICROSOFT AZURE

This is one of the most exciting times for anybody who works in technology, and in computing in particular. What we have today is

some of what we have imagined 20 years ago: little variables some of us even have imbedded in our bodies. I am sure that in the future we will see drones delivering packages to robots, software and chips controlling our critical infrastructure, software and satellites robots on the moon and even Mars. Ubiquitous computing in all its glory is upon us.

In the last few years, innovation has become absolutely outstanding – almost every person, business and organization is looking at technology inadvertently, but is most likely to get the extra-edge by embracing technology. Along with that comes cyber crime, and it's not unusual. When we invented steam engines and railways, there were the great train robberies; When we came up with the postal and the mail system, we had mail fraud; and so, in that sense, the new technology "invites" the good and the not so good. Cyber crime offers some unique new challenges: you can be sitting in a remote location somewhere in the world and hack into a satellite up in space or attack across the globe, and it is extremely hard to defend against those attacks.

While the environment is challenging, I think technology itself gives us the best hope in combatting these threats, and I will take you through a very quick set of technological elements that I think hold the most hope for us in this matter. We are talking about collaboration, but I think our defenders and responders are also our big hope, and give you a quick tour of my top picks; most of what I am going to talk about is available technology, some of which is already being used, while a few of those things are more aspirational.

To organize my thoughts about the problem I use a framework which I believe that is more familiar with the security community: to protect, to detect and to remediate. There are different possible combinations, but I use it to organize ourselves. The other reason why I think this framework is useful is that I am beyond this controversy – whether protection is overrated and detection is where all the funds should be or not. I think the innovation across all three spectrums has to come together, and I think that first you have to look at all three and innovate in all areas in order to have a real fighting chance to get ahead of the cyber criminals. In Israel, especially if you are an entrepreneur, we look at it in the broadest sense, because there are interesting opportunities in each of these areas.

I will start with protection. Some of the things I am about to mention are relatively new. Just recently, intel announced what is called "control flow enhancement technology", basically a shadow stack, which eliminates a whole class of problems that arise from Return-oriented and Jump-oriented programming. It is one of the most prevalent software vulnerabilities that hackers exploit, and in a couple of years, as the chips go to mass-market, I believe it has the potential to eliminate a whole class of problems that have plagued us. We made progress with data execution protection, such as static and dynamic analysis, but this technology really goes to the source of a fundamental class of problems that plague our software.

Equally exciting to me is the virtualization and additional protection boundaries that hardware is creating for us. Along with that, of course, we need an operating system and firmware to build a whole stack, but the use of Trusted Platform Module (TPM) to store passwords that are protected even against the administrator on the machine stealing them is a fantastic innovation. Along the same lines, we used this additional protection domains to even protect code, so that it is not tampered with or stolen or even looked into by administrators, and the same technology can also be used to establish new forms of trust between the customer and the cloud provider; and while trust itself is an interesting artifact, it is indeed impressive security that even an administrator level breach is not going to take away credentials or the special IP of a customer. This exciting technology is already being used, not only in Azure, but in several other places.

Along the same line, there are also root kits and back doors. We are making great progress in the industry around secure boot, which allows us, even before the operating system gets initiated, to measure how it booted and detect the class of problems. This is called attestation and integrity for large scale servers, such as Azure and every other Cloud service, having only signed code run on our back ends. This is a fantastic advancement, which will make it much harder for malware to get into servers. And finally, Micro-OS is minimizing the footprint of the attack surface itself, and offers great hope.

I would be remiss not to talk about all the possibilities that encryption can offer us. On one extreme end, you can have a very tight protected domain, which is not accessible even to the operating system or the administrator, where core can run and you can encrypt, decrypt or

transform your data within that region without any leakage. On the other hand, there is the homo-morphic encryption, which is the holy grail, but there are steps being taken where arithmetic operations search, and even machine learning models are being built where the data is always encrypted. Secure multi-party computation and collaboration is absolutely the new norm of doing business, and secure multi-party computations encryption has great hope, although while trust and privacy are important, security is an absolute killer application that exploits all of these things.

On the detection front, our point of view is that if you look at the kill-chain there is rarely a single bullet that goes to the heart of the organization. If you follow how the sophisticated attacks happen, you see that they use a variety of different things: they follow the normal kill-chain process, casting the widest net across your enterprise to actually detect malicious activities is one of the key innovations. We look across end-point clients, servers' identity, user behavioral analytics, network, and we find pretty high correlation between software crashing and that piece of software being under attack. There is much research being done, and this is another example looking at a multiple inputs and multiple signals and being able to correlate across them.

There is much innovation in big data, machine learning at Cloud scale; we use it regularly, and in a very interesting way, across the identity stack and across Azure. There are great opportunities there, and while we have had years of work on correlation, correlation is still important, and anomalies in base lining – and specifically looking at anomalous behavior – holds great hopes for us to improve the detection even further. The most important thing for me, of course, is the Cloud effect. From what we see happening to one tenant or individual in the Cloud, we can learn and apply to literally millions of tenants and users, and I know that many anti-malware products use it. I believe that the cloud effect gives us some immense power in having better detection.

I think that in Israel, deception is very widely used, and many startups are working on it. Deception is a very interesting technique, and if you build it into the stack, the operating system and the application, you will definitely get more out of it. Honey pots are, of course, another great technique for deception. One of the fields in which I think the opportunities are still ahead of us is remediation. If you assume

breach, you will have the issue of cleaning up and recovering. There is much low-hanging fruit that we need to automate, such as rolling-over keys or certificates, making sure that suspicious activities lock out the account, and let the users multi-factor their way back and re-set their passwords. Every time you design a new app, you have to segregate its state. In the worst-case scenario, if you are suspicious about something going around, block the VM and rehydrate your app. And, of course, there is much more we can do there.

Another beautiful thing is that we learned how to build Cloud services with a set of cloud principles. We partition, so that if something was to go wrong, only a minimal number of users are impacted. We also learned how to build Recovery-oriented design into the stack, which is also an extremely important thing that will help security. Wherever you have high-impact operations like deletion of records, soft delete is fantastic thing. We learned that humans make mistakes, so we built soft deleting, and I think those kinds of techniques are going to be very valuable. And then you have multi-party access control: if you are going to wipe out a big amount of data, make sure that two or maybe three individuals sign off before such an operation can take place. These are some of the things we do, but I still think that the biggest opportunities in remediation and recovery are still ahead of us.

I also think there is a huge opportunity in collaborations. Threat intelligence is the easiest thing to collaborate on, but I think there is work to be done in terms of attribution. Knowing the adversary, who is doing what, and how to react to it is an immensely important thing, and if the big software players were to focus on collaboration, we would have huge opportunities to go after the really tough, big criminals to start with. Easier said, hard to do, but I think that at the end of the day, the economics itself will take care of it; we will figure out how to collaborate rather than to reinvent everything on our own.

As a Cloud vendor, I see great opportunities ahead of us in using simulation at Cloud scale with our red team, where we can really practice on response to an attack, and how we recover from it. But what about the modern defenders? I think – and I credit this to my two colleagues, John Lambert and John Warthon – that our defenders have taken a very interesting path, where we can assume breach but don't look at it just as assets to protect. We don't really worry about incidents, but instead we look at the adversaries. Finally, I really do

think that it is time for us to be full-stack defenders, not point-solution defenders, or look just at leering at more solutions; we really have to understand the whole stack, because in it lie the best opportunities ahead of us.

I am optimistic, and believe that technology itself has the best hope for us in keeping ahead of the situation. We have to look at the whole stack and the entire framework of protect, detect, and remediate, and obtain the best arsenal to stay ahead, and the modern defenders will be a key element in every company's future.

NADAV ZAFRIR, CO-FOUNDER, CEO, TEAM8

Over the years, I have had the honor to meet some very interesting people – heads of state, leaders of enterprises – but the other day I was really excited when the Prince of Nigeria asked me for help personally. This was not just a courtesy call, but a cry for help, and I had thought, how many people in have had the same honor as I had? But if you look at it a little closer, does it still look legit? Most of us have a PayPal account. When I get into my PayPal account and there is a new address, and I want to check if it is legit or not, what do I do?

I don't want to talk about phishing attacks, which is probably at the low end of the totem pole when it comes to breaching your end-point devices; but I do want to talk about the fact that once somebody does breach your end-point, in many senses now they are you. Because now they can impersonate you, and whatever you can do – they can do too. If they are somehow able to penetrate your end-point and circumvent all of the defenses we keep talking about – they are in. I think that, in many ways, this happens because human nature is to make mistakes, and so we do; which is probably a good thing, because mistakes also allow us to innovate and evolve and get better.

If human nature is to make mistakes, machines are naturally imperfect, and these operating systems – which have begun as something that operated a handful of tasks that were pretty straight forward and clear – have evolved in this monstrous monolithic general purpose system of everything that controls everything that we do. They contain hundreds of millions of lines of code, and they are supposed to be perfect because they are designed and built to be perfect. Personally, I believe that in this, we are failing miserably. There is some sort of

connection or bonding between men or women and machines, and in my opinion, this connection between people who make mistakes and these imperfect machines is probably the perfect petri dish for disaster when we speak about our operating systems. For that reason, I think we have to start designing for failure.

I am not talking about the concept of security or cyber security by design; I am talking about a phenomenon that has been around for many years, of critical infrastructure that has to be reliable, and that is designing for failure. As soon as the ship was invented, shipwreck was invented with it, and the question is: why? What if we design the ships in a way that if there is a spill in one area that doesn't necessarily mean that the whole ship has to sink?

Think about nature in terms of diversity: polyculture in nature is where you have different crops at the same area, and in modern agriculture we have started to adopt monoculture, meaning you have hundreds of thousands of acres of exactly the same crop. And guess what? That is not sustainable. Over time, this method kills the soil, plus, one pest can kill all of the crops. We did it because it was much more efficient, but modern agriculture now is starting to adopt polyculture concepts from nature, and we find that it is not only more resilient, but also more sustainable, making it more efficient and more profitable.

Talking about operating systems, I think we see vendors who are doing it as well, or taking the first steps. Take Apple, for example. Nowadays, in iOS, the data for your fingerprint is not stored in the general purpose bloated monolithic operating system, but in a separate hardware enclave, so even if somebody does manage to breach your end-point, they won't have the data for your fingerprint, which makes sense. Microsoft Windows 10 takes this to the next step, where you have sort of a designated side-by-side operating system that stores your credentials, so that it is impossible to do things like passing the hash or Cerberus ticketing, for example. I think these are important steps that might win us a couple of battles, but not the war.

So how can we win? I think – and this is heartbreaking – that we have to break up with our operating systems. I think that this inseparable bond between man and machine should be broken, because we cannot expect people to stop making mistakes, and we shouldn't be expecting our machines and operating systems to be perfect. What I mean is that

we want to have an environment at our end-point, where we can use multiple operating systems from multiple instances, all at the same time, and I think it is possible to do this not only seamlessly from the user, which has obviously been an impediment until now – but also something maintainable for IT.

The reason is in terms of our hardware: there has been tremendous progress over the last two decades. If we look at the RAM at the end-points, for example, two decades ago it was around 8MB, and now it has reached 8GB and even more; Storage space increased from 1GB to 1TB at the end-points; once we used a single slow processor, while now we are using multiple processors that are much faster than we could have imagined twenty years ago. That enables virtualization that allows us to use the Cloud, and all of this together is a pretty good ground for breaking up with our operating systems.

Imagine that you have not one, but two or three instances of windows operating systems alongside the same end-point, with a couple of instances of Linux, working together simultaneously, seamlessly to the user and to the IT. You know there are a thousand ways to breach a network, and I am not saying that by breaking up with our operating systems attackers are not going to breach our systems. I am saying, though, is that by doing this, we might dramatically lower the probability that this specific breach into our operating system will create a systematic devastating conclusion.

DR. DOUGLAS MAUGHAN, CSD DIRECTOR, HOMELAND SECURITY ADVANCED RESEARCH PROJECTS AGENCY, USA

When you think about innovation, most people think of government as slow, filled with antique legacy systems. Recent reports said we still have COBOL and mainframes in the US government. Government is also not flexible, but a structured environment. Is the government a great customer? I would argue that it is; if you can get in the government door with your technology, the government is actually a great customer. However, most people don't see government as an innovator. I am going to give you an idea of some processes that we have put in place in the Department of Homeland Security Science and Technology Directorate, that show that government can be innovative and can do things very differently.

How do we work in the Science and Technology Directorate? we are a research organization that is doing applied research, development testing and evaluation, and transition of inter-commercial products. We are not a basic research organization; we are trying to commercialize technology out of the research pipeline, and we take requirements from many people, both within the White House and other government agencies. DHS is a large organization, 240,000 people strong, across the globe. We get requirements from all of those operational components. We get requirements from our inter-agencies, and from a number of other government agencies. We also get requirements from the private sector. I am going to talk about two engagements with the private sector that we are doing in critical infrastructure. We are also working with our state and local first responders, they are the front lines of cyber security nowadays. In addition, we have our international partners, Israel being one of them.

Let's move to the finance sector and the Transition Project. We needed to do sector-specific resilience, and what we are doing with the finance sector is a project that tries to leverage government-funded research, as well as commercial products, and bring it into the banking and finance sector. It is a partnership between DHS Science and Technology, the Department of the Treasury – which is the sector-specific agency, several banks in the US, and a customer or a performer who is running a consortium that small companies, large companies, and labs can join, if they have a technology that might be of interest to the finance sector.

The finance sector has identified five major areas, which we call the "hot spots" or the "sweet spots": software assurance, dynamic defense, network characterization, malware detection, and inside threat. Those are the five areas we are focusing on, and we are leveraging over $60M of government funding, another $20M of national labs, as well as commercial products, where we bring those products into a testing and evaluation environment with the banking and finance sector. Again, the goal here is to bring technology to the critical infrastructure owners and operators. You can see the customer buy-in – we have several large US banks that are already participating, and they are there to give us strategic direction. They are the end-customer, their job is to help us understand the technology and how it will fit into their

operational environment. Last but not least are the starting tasks, which are really about network security and network identification.

Our second critical infrastructure project, which has been going on for quite a while, is with the oil and gas sector. We have a joint collaborative research project with five major oil companies, ExxonMobil and Chevron in the US; BP in the UK; Shell in the Netherlands; and Total in France, and this is an international collaborative research and development project. This is a very different engagement than most people would think of the way government is involved with the private sector: we all put money on the table, they decide on the projects, we help them run the projects and then deploy the technologies out into their infrastructure.

The third process I wish to discuss is something we have initiated in 2014. Over the last three years we have funded approximately $95M in various technology areas. This is different than other processes because the review board was made up of international government partners, so in fact some of our partners from the Israeli National Cyber Bureau were on the review team and involved. Another difference is that we are allowed to fund international researchers, so we actually fund entities external to the US; so not only do we have government employees on our review board, we also have international researchers that submit proposals and can actually get funding.

We are in the process of early planning between us and the Israeli national cyber bureau, for a joint call in 2017 between the US and Israel, where the requirement will be a joint proposal from a US research team and an Israeli research team. More information about that will be available in the future. Additionally, we are in discussions with various international partners to promote the creation of an R&D consortium from the governments' standpoint. Every government has the same problems, and the idea is to document them and work together; solutions are not national, but global.

As for the fourth process: The Department of Homeland Security opened an office in Silicon Valley, and I am leading that initiative. What we are trying to do is accelerate technology coming from innovative start-ups, and bring it into the operational environment of DHS. In the past, we relied too much on larger companies to bring that technology

in, and so we are trying to do something similar to venture capitalists, when the goal is to bring technologies into the department.

For that purpose, we are doing three things: the first is educating people about DHS. What most people know about DHS is only what they see at the airport, TSA customs and border, but DHS is a much larger organization. We are trying to educate them about the mission that we have. The second is to fund start-up companies with new technologies that will be helpful for us. The third thing is to test those technologies with real customers. If you are an entrepreneur, trying to find your first customer is one of the hardest things you can do, and we are trying to make that easy by being that first customer.

As I mentioned earlier, our goal is to accelerate new technologies into DHS and into the directorate. Where do we fit? We have discovered, as entrepreneurs know, that between receiving accelerator money, incubator money and a VC round A, there is a valley of death for a start-up company. It usually takes 1-3 years, and this is where we come in: we fund start-up companies that are stable enough; that have had previous funding, but are still young and flexible enough to change what they are doing for DHS purposes. We are looking for companies that have a commercial product. It has to be commercial, because we are the government and we are not going to be a big enough market for you; we will be a secondary market. However, we will fund product development to get these products into the market faster.

We are not looking for people who are willing to change their direction just to try and get government money, it has to be in a certain space; and the other innovative thing we have been doing is not taking equity or IP. It is your IP, your ideas, and we just want to help you get them into the market. The way our process works is very different than what you might normally think of as government. Most government processes in the past have taken 9-12 months to get a contract in place, while we use a special authority, called Other Transaction Authority, and a Solicitation that goes with it. We publish, people can respond to the call with a solicitation, we review their applications, and invite some of them in for an in-person pitch before awarding them a contract.

The other transaction contract is not a traditional, government-based contract. In our first process, we went from the initial call to the first award in 60 days – which, for government speed, is very good, and

just as fast as the venture world, and sometimes even faster. It is an interesting model with four phases. The value proposition for a start-up company is $800K over a 24-month period of time; that is our maximum amount of money and our maximum time period. It can be faster than that. What we are doing is Proof of Concept, a beginning prototype, a mature Proof of Concept pilot, and an initial appointment with a customer over the course of that time period.

Our first call was in IoT security. Everybody knows about Internet of Things, and about its security problems. Of the hardest problems that we could try to solve, we picked three: identifying IoT devices on your network and in your environment; authentication of those devices, how to ensure that those devices that are in my network are in fact authentic; and the update problem – how to update these devices in a secure manner, so that they don't become legacy systems? From a DHS perspective of critical infrastructure protection, everyone has the same problem.

Even though we say it is a Silicon Valley program, a national program, it is actually global; we can take applications from international companies. We have been in business for six months and have so far reviewed 34 applications, invited 9 pitches, and have made 4 awards with one more in process, all in a process that takes, from start to finish, no more than 60 days. We post our call out there, usually on certain topic or areas, for example the IoT mentioned before, wearables for canines to help monitoring capabilities for the DHS dogs in airports and other places, and so on. We frequently publish such calls for applications, as we invite everyone to participate.

3RD SESSION: BUILDING CYBER, PROTECTING INFRASTRUCTURE (PANEL)

KIM ZETTER, INVESTIGATIVE JOURNALIST & AUTHOR, WIRED

I started my journalism career in Israel many years ago, so it has been a bit of full circle for me to now write the book on Stuxnet which was,

of course, about an operation that was rumored to be conducted by two countries, Israel and the USA. Some say that Stuxnet has broken three paradigms. The first was the myth was that cyber attacks were only about information: stealing information, degrading information, changing information, and preventing access to information. Stuxnet was not even about causing damage to the systems that it infected, but about jumping from the digital realm to the physical realm and causing physical destruction of systems that the computers controlled.

The second paradigm that Stuxnet broke was the idea of what we think of as a computer. I have been covering cyber security since 1999, and control systems were never on my radar. They should have been, but I think that most of the security community, outside of a small niche of people who are experts in industrial control systems and security, weren't really focused on these as computers, things like programmable logic controllers, and remote terminal units, so this was a whole new area that was opened up, not only to us, but the hacker world as well got introduced to these systems.

The third paradigm that Stuxnet broke was the idea that only systems that are connected to the internet were targets of attack. Now, this wasn't a surprise to people who work in cyber security, since, for example, there had been attacks or infections conducted through USB sticks in the past. However, primarily the focus was on systems getting infected and attacked over the internet, over some kind of connectivity – Bluetooth, Wi-Fi. This really made it clear to everyone that systems that are heavily secured and guarded, even behind anti-aircraft systems and guns, could be accessed with a digital attack.

Stuxnet was the first attack that we know of that leapt from the digital realm to the physical realm, to cause physical destruction, but it wasn't the first one that actually occurred. There was a Proof of Concept attack that was conducted by researchers in 2007, called the Aurora Generator Test. This was a 27-ton generator retired from the oil fields in Alaska, and the test took place at Idaho national Lab, a government lab. The premise was that some researchers started wondering if it would be possible to cause physical destruction with nothing more than digital code; would it be possible for remote hackers in Russia, North Korea, China, or any other country, to send digital code that could leap from the digital realm to cause physical destruction? The Aurora Generator Test was targeting the protective relay. The

protective relay on the grid is designed to detect when systems are getting into a dangerous zone. For example, the electrical grid in the USA operates at 60 Hertz, and all of the equipment that is connected to the grid has to be operated at the same frequency, otherwise it can cause damage to the grid or to things connected to the grid, such as the generator. The protective relay is designed to detect when something like a generator is getting out of sync with the grid, and if the frequency increases, the protective relay triggers the breaker to open, and disconnects that generator from the grid.

The Aurora Generator Test attack, which was composed from only 21 lines of code, was designed to subvert the protective relay and trick it into thinking that an out-of-sync condition was actually a healthy, appropriate condition, and instead of opening the breaker, the protective relay would actually close the breaker when the generator is out of sync. Those 21 lines of code, which constituted a cyclical attack, caused the protective relay to open the breaker first, and when the breaker opened the generator, which would then speed up the frequency because there was no pushback from the grid against it. Then the code would tell the protective relay to close now, even though it is out of sync; it would open the generator, which would speed up again – close, open, close, and so on. It only took three minutes to destroy a 27-ton generator. They could have accomplished it in fifteen seconds, but the engineers built in some pauses into the attack, so that each time the generator got reattached to the grid, the safety engineers would be able to check that everything is okay. What happened was that the generator produced too much energy, hit the grid, came back, and attacked the generator.

There was another Proof of Concept attack that took place at the DEF CON hacker conference 2015, which involved a 50-gallon barrel. The idea was that this kind of attack could be conducted against a chemical plant. Jason Larson, a former worker at the Idaho national lab, designed an attack that would vacuum-pack the barrel while simultaneously increasing the heat inside the barrel. When the barrel collapsed, there was a shockwave in the room. When you have an attack like this, which destroys barrels in a chemical plant and causes a chemical spill – and, of course, can work on multiple barrels – you can destroy such barrels inside of a plant, and might cause a toxic chain reaction.

After Stuxnet was discovered in 2010, everyone in the security community – particularly Ralph Langner, who was one of the researchers who helped take apart Stuxnet – predicted that we were going to see a lot of copycat attacks, and we haven't. Other than the recent blackout in Ukraine, which was not a copycat attack, and a reported attack against the Turkish pipeline – although there is a major dispute about whether that was actually a cyber attack – we haven't really seen attacks on critical infrastructure that have caused any sort of real effects. This makes one wonder, are there any other incidents out there that are happening but aren't getting publicized?

We looked at what Stuxnet did, and we looked at the Ukrainian firmware upgrades. When the attackers targeted the Ukrainian power distribution centers, they opened the breakers, but to prevent the systems from being brought back up remotely, they overwrote the firmware on the remote terminal units that were out in the field. That way, the operators couldn't restore and close the breakers remotely, but had to send people out into the field to physically close those breakers. To my understanding, that manual capability that exists in Ukraine is quickly being eroded in the USA, so when you are automating system, it is going to be much more difficult to bring them back up.

One of my main two concerns, in terms of the current situation, is the firmware issue, that the firmware on devices is not secured, and so it can be overwritten. My other concern is related to an attack that we took place in 2012 against a Canadian company called Telvent, a third party control system. They have many customers, and they install control systems in plants and then they monitor them. In that attack, the hackers got into the program files, and if you can get into those files and introduce your malicious code there, it is going to get introduced to those clients through a trusted third party, which is exactly what happened with Stuxnet. Stuxnet was targeted on contractors who worked at the facility at Natanz, and they carried Stuxnet into that facility.

In the USA there are sixteen different sectors that the government defines as critical infrastructure, including – to the surprise of many – motion picture companies, such as Sony. A report came out in the USA in 2014, which examined what it would take to bring down the grid nationwide, which is one of these critical infrastructure sectors. The report indicated that if you could take out nine key transmission

substations, out of the 55 that exist in the USA, it could cause a nationwide blackout, possibly for weeks and maybe months. It also depends on what you destroy – if you destroy equipment like the Aurora generator, which is a relatively common piece of equipment, it can be replaced fairly quickly. However, if we are dealing with the destruction of a generator that is on the electrical grid, these generators are custom built, and can take a year or longer to build again. Therefore, if you can take out or destroy those generators, it would take a substantially longer period of time get the system back up. These problems are of a global scale, as this scenario is applicable in many countries worldwide, and this is something that should worry us all.

MARK GAZIT, CEO, THETARAY

A question that often comes up in discussions is, why we don't see many Stuxnet-like attacks on critical infrastructure in recent years? First of all, such attacks do happen, but what distinguishes organizations like Facebook or Google from others is that if someone takes them down, it is evident to everybody. When there is an attack on critical infrastructure, what the average user will experience is usually just an outage. Most times, it will not even be published or disclosed as a critical infrastructure attack, which I believe to be the right approach, because you don't want to let the hackers know that they were successful, so in most of the cases it will be identified as a malfunction.

Another reason that we don't witness many such attacks is that they are extremely difficult to identify. Stuxnet wasn't about breaking into a system, or about viruses and network security; it was about changing the speed of the centrifuges. To identify such an attack, you need to analyze the speed, the velocity, and the pressure of the centrifuges, which most organizations cannot do, or cannot identify as a cyber security attack; they just don't always know that they were victims of such an attack.

When referring to Stuxnet, we are dealing with something that is completely transformational, it is a world of unknown unknowns. If, allegedly, governments did it, then antiviruses are rendered irrelevant, because it is a zero-day attack, which didn't exist before. You can't use firewalls, because the Bushehr nuclear power plant, in which the attack took place, was inaccessible via network. Therefore, you

need to analyze a new breed of information that you have never seen before, and the problem is that the amount of information is becoming enormous, to the point that you can't analyze it all anymore.

General Electric introduced Predix, a Cloud-based platform-as-a-service (PaaS) that connects all the devices, but suddenly even that is not enough to digest the amount of information. For example, one 30-minutes' flight of a Boeing-787 airplane creates 2TB of data, which is the equivalent of 400 libraries of congress. You need to analyze it in real-time to identify cyber security attacks, such as Stuxnet. What do you do? How do you deal with it when existing solutions, based on rules and patterns and such, don't work, because you don't have any existing and previous knowledge? You need to find a needle in a haystack. When relating to critical infrastructure, one real-life example that we face is ATMs.

An ATM is just a SCADA device. Its structure is very similar to that of a nuclear facility in Iran, because it is basically a computer running windows XP, along with a few motors that get SCADA commands. Historically, if you wanted to steal money from an ATM, you had to use fake credit cards or skimming devices. Today you can break into the backbone of the ATM: you send SCADA commands to the motor, which starts spinning, and then you send another SCADA command to the actuator, which opens the door, leading to the very interesting phenomenon of money coming out of the wall. All you need is what they call "money mules", criminals that will collect the money. This may not sound critical, but if we are talking about a country in Latin America, with 6,700 ATMs, all of which were hacked at the same time, that becomes a public unrest issue, which needs to be solved.

We believe that there is also good news. Today, with the advancement of cyber security attacks, and with the ability of hackers to use or abuse machines, if you want to launch an attack, all you need is a few people that will use bots to take over 100 million computers, which, in turn, will be used to carry out the attack. The good news is that those computers can also help us, when you have the right algorithms, and when you know how to look for these unknown unknowns.

We strongly believe that in this new world, you are not looking for a needle in a haystack, but rather a needle in a needlestack, because they all look the same, yet one of them is different. Human beings are

unable to identify those attacks. Luckily, we do have machines, and we believe that with Cloud platforms like Predix, with analytic machines that can identify those attacks in real-time and alert people, at the end of the day, this plot will have a happy ending. History shows that eventually, the good guys win. Bad guys move faster, but good guys win in the end.

We live in an interesting world. There are cases, such as the Sayano-Shushenskaya dam in Russia, where we are not sure whether or not an incident was a cyber attack, and if so – who to attribute the attack to. The Sayano-Shushenskaya dam has a 2-ton turbine, which is very different than the centrifuges in Iran, as well as a computer that was supposed to deal with vibrations, and as far as we know, someone broke into that computer. This computer suddenly stopped detecting vibrations, causing harmonic movements that led to a 2-ton rotating machine coming out of the pit it was stationed in, thus destroying the dam. Was this a cyber security attack, or was it something else? We don't know.

Another case is the BlackEnergy Trojan attack in Ukraine. When Russia tried to take over Crimea, they had to shut down communication with the mainland; everybody in the world knew what is happening, except for the Ukrainians in Crimea, because no internet data was coming into or out of Crimea. The reason for that was a large-scale BGP attack, causing the traffic to be rerouted to Russia. Later on, the Russians allegedly decided to shut down the power grid; they took over the systems using Command & Control computers, and sent commands to shut down substations, as well as the UPS grid. They modified Ethernet-to-serial converters, which were required for normal network operation, because some of those machines don't even speak modern protocols, but rather something called "serial protocol". We know that the operators saw the mouse cursor moving on the screen and clicking icons, and they were just helpless.

Personally, I believe that it happened that way because Russia wanted everybody to know that they were the ones who did it. They could have just shut down the system without making the cursor move on the screen, but I think somebody there wanted to show off, and prove that they could do it. In this case, we have real evidence that this disaster was a cyber attack, but in how many cases attackers didn't move the cursors, and just shut down the sub-systems in a way that was

classified as yet another malfunction? There are many bad things about wars and the crisis between Russia and Ukraine, but one good thing is that we could witness cyber warfare in action, one where I believe one party wanted to be discovered in order to threaten the other party.

What I am concerned about the most today doesn't necessarily involve a specific technology, whether its firmware or financial institution software written in ancient languages like COBOL. I am concerned about the availability of tools. There is a concept in the world of espionage, called NOBUS – nobody but us. The idea is that governments tend to think that even if they have the ability to discover vulnerabilities in a system, nobody else will find out how to do it. This is true for almost any government.

The problem is that there is a leakage of technologies to the hands of criminals, and a great example for that is a company called Hacking Team, which created amazing technologies that many intelligence agencies all around the world were using. Their technology allowed them to affect almost any mobile phone, activate cameras, voice, etc. Unfortunately, somebody broke into the Hacking Team's network, and made all those tools public, available to everybody. This is similar to a truck full with RPG missiles that suddenly falls at the side of the road, and every criminal, every terrorist can get those tools, which are military-grade warfare tools. This is my biggest concern, and one of the reasons that led me to establish ThetaRay.

I believe that today crime becomes a very profitable opportunity. You can take over hundreds of millions of computers and make some money, sometimes big money, and nobody can catch you or even attribute it to you. I think those people make the world an unstable place, and that we all need to join hands and fight very hard to make the world a much safer place.

RICHARD PUCKETT, SENIOR DIRECTOR, SECURITY OPERATIONS & CYBER INTELLIGENCE, GENERAL ELECTRIC

When we think about the systems and services that provide critical infrastructure, we talk about the grid a lot, but critical infrastructure is comprised of a lot of different areas: health and emergency services, water purification, hospital environments, and others. These domains are defined, and what it takes to both attack and defend them, as well

as the consequences associated with them, are somewhat different than what you see in your traditional IT spaces.

When an IT system is taken offline, sometimes the consequence of that is a loss of your information, or maybe exposure of your banking credentials. Also, the recovery states that occur as a result of that are well-pathed and well-defined. If your banking credentials have been compromised or your credit card exposed, the banks tend to issue you a new card very quickly, the debt is erased from your account, and you are back in operation. However, in critical infrastructure we think a lot about the consequences.

When we think about the consequences of a failure, for example, when a system goes offline, it is very visceral; it can be a loss of power in a home, an impedance of emergency services, or the loss of connectivity for your cell phone. When we think about design and defending critical infrastructure, these are the biggest issues that are pressing us today. We tend to talk about the legacy issues of Microsoft quite a bit, and how they have to have all this backward compatibility, and how difficult it is to create new platforms. They have a very challenging problem, because people have yet to see how difficult it is going to be to advance in some of these new domains of critical infrastructure, all while bringing along the long tail of legacy.

There is equipment in the power grid today that can be 30-40 years old, and when it was designed and deployed, it was never intended to be cross-connected or connected to the internet, whether directly or indirectly. These environments come with a legacy issue that we have to figure out how to navigate, as we are creating these new capabilities in critical infrastructure to optimize and try to make them safer, which is a really big design component for us. Also, there is the issue of how to make them interoperate. The newer systems that we bring to bear can have all the great security features, but to make them interoperable with legacy sometimes means a downgrade of security, which is often a big challenge. If you take the example that was given around Stuxnet, it was actually taking advantage of not only what the centrifuges were doing, but also the clear-text protocols that made it easy for a man-in-the-middle (MITM) attack to work.

You have to think about those things and about the ecosystem you are defending in critical infrastructure, and that is a huge part of

the story today. This is a good topic to bring forward, because in that disruptive trend, we are moving towards more software introduction. In our company, we talk about where Big Iron meets Big Data, and where the software bridges that chasm between the two. There is much innovation that is needed to help defend these environments, and that is not only when we bring these new things to bear, but also as we think about cross-connecting legacy.

There are two ways to think about the lack of publicity of cyber attacks on critical infrastructure. The first is on the nation state tier, like with the recent announcement about Operation Dust Storm, the attacks on Japan's critical infrastructure. A company called Cylance uncovered that attack campaign, and it is a very interesting case, because it was a 5-year campaign of broad-reaching attacks. They used a wide range of attacks, everything from spear-phishing to zero-day Flash and IE exploits. You have to look at such attacks from the standpoint and the objectives of a nation state and what the attackers may be targeting.

I think we tend to talk a lot about Stuxnet, as it was a watershed event in terms of visibility. However, when you look at some of the recent discoveries concerning Flame, DuQu, Gauss, Shamoon that hit Saudi Aramco, and others – some of those were our customers, and the outages were quite severe. At the nation state level, we can also look at what happened between Russia and Georgia 72 hours before Russia invaded Georgia; it was all cyber: everything from banking to telecommunications was hacked to create disruptions. We currently think about cyber as the fifth dimension of warfare, along with land, sea, air, and space, with cyber becoming a doctrine of warfare and a political tool of nations.

The second way to think of this issue is the cyber criminal world; it can be hacktivists, insiders, non-state actor groups, and so on. The place in which those two arenas meet is a very interesting place in the underground economy, where you can even see more pedestrian forms of attacks like ransomware: CryptoWall, Lockey, and many other types of ransomware that are hitting hospitals today, with very effective means. The hospitals are paying, because their in-patient records are being encrypted. MedStar was hit, and so was Hollywood Presbyterian, among others.

However, the most effective piece of malware across all critical infrastructure today, which has created the most disruption at the most generic level of human-machine interface (HMI) and SCADA, is no other than the Conficker worm, sometimes referred to as the "common cold" of the internet. The reason is that legacy infrastructure has Windows CE, XP, Windows 95 Embedded, and the worm can hit things like ATMs, which have no defenses, and it still manages to create forms of disruption that may not make it to the public eye, but they are still problems that need to be remediated.

We are in a constant race condition that is not going to stop, and in fact it is probably going to accelerate, and I think that there is the issue of accessibility. Five years ago, IoT and ICS weren't even on the agenda of mainstream hacking and penetration testing research conferences, while now there are entire conferences dedicated to it. I think that there is a race condition: on the one hand there is the positive side of exposing vulnerabilities for correction, to keep things safe, while on the other hand there is the negative side, where the same exposure of those vulnerabilities in the hands of non-state actors, or in the hands of people who are not thoughtful, can have very catastrophic consequences. Sometimes those consequences occur because the actors are not careful, and sometimes they are intentional and malicious. I tend to stray towards the positive, and say that the race condition is in our favor when you have a large community of people that can focus on creating effective solutions to help improve the problem, rather than take advantage of it for destructive means.

TERRY ROBERTS, FOUNDER AND PRESIDENT, WHITEHAWK_

I would like to refer to the issue of why we don't see or hear about more Stuxnet-like attacks or attacks on critical infrastructure in general. I look at this issue from both viewpoints of a former national security professional and a current cyber intelligence professional. What I believe is that simply because something hasn't been done again, it doesn't mean that it isn't being planned at the moment, or that there aren't targeting folders available; it doesn't mean that this isn't something that state actors or hacktivist groups don't have ongoing. I always imagine the worst-case scenarios, and that we should be preparing for the worst. In my opinion, we should take this area very seriously, because when we weaponized software to be able to get

to critical systems, it became both a safety issue and a warfare issue at the same time.

Another aspect I wanted to bring up is how we should think about potential hacking of critical infrastructure, and how we should become problem-solvers in this important area. Without getting into too much detail, I think it is less about information sharing and more about cyber threat intelligence sharing. It needs to be done in this arena, within the sectors, at the next level up; it needs to be done across countries, because this is not something that is limited to one or two countries; everyone who has these critical systems is impacted. We are all at risk, and therefore we must do today anything we can to raise the bar in automated sharing, analytic sharing, and campaign sharing.

Every week I meet with 2-3 incredibly innovative cyber security companies as part of my business, and there are currently some great asymmetric approaches to critical infrastructure vulnerabilities. There are Israeli companies, German companies, USA-based companies, and so on. Some of them are creating encrypted techniques for the control systems, some are putting in place new approaches to capture the adversaries as they come into your system, while others are doing assessments, so that you can fine-tune where your critical vulnerabilities are. We need more companies, more innovation, and more research focused on this space.

***

Looking at a real-life example for the potential damage and outcomes of a nationwide cyber attack of critical infrastructure, the Russian cyber attack on Ukraine was a very scary combination of various types of attack. If someone was to shut down the North-East power grid in USA for a period of 12-48 hours, and also combine it with other malicious activities and attacks, significantly reducing the authorities' ability to respond, to communication with each other, with the population, and with the world, as well as their ability to help people – that would have been an extremely terrifying situation. For this reason, among others, thinking about cyber attacks on critical infrastructure is such an important issue.

I am very concerned about countries that don't properly prepare themselves to a nationwide attack. In late 2014, the USA government published the presidential directive 21, which revolved around

interagency roles and missions in cyber space. It discussed who is responsible for what, how to put that in place, and strategies regarding effective communication across the government and with the industry.

I am not saying that we can't prevent a large-scale cyber attack, but if one does happen, we have to be able to very effectively respond and mitigate, and you can't do that if you don't have all the lines of authority, communications, policies, and threat intelligence sharing at speed. All of our respective nations need to get their act together, and work with the industry to put those frameworks in place.

DR. DIMITRI KUSNEZOV, CHIEF SCIENTIST, NATIONAL NUCLEAR SECURITY ADMINISTRATION, DEPARTMENT OF ENERGY (DOE), USA

I would like to start by providing a little context about how we approach the energy critical infrastructure control systems at the Department of Energy. To do that, we have to take a step back and think about cyber security in a much broader context. The Department of Energy is an interesting collection of authorities, responsibilities, and capabilities that converge on complex systems and enterprises – we start at one end with power management administrations, we own transmission wires for about 10% of the country's electrical transmission, largely tied to hydroelectric power. The Federal Energy Regulatory Commission is part of the Department of Energy that is in charge of regulation in the sector. Under that, we are the identified department responsible for the energy critical infrastructure in the USA, and the tool set we have includes laboratories, such as the Idaho National Laboratory that ran the Aurora test in 2007.

The department has a workforce of almost 100,000 scientists, engineers, and technicians, spread around the country, largely at seventeen national laboratories. In those locations, we cultivate expertise in broad sets of missions that facilitate a lot of crosstalk, allowing us to attack very complex problems. We are typically an agency that partners across the government, as well as internationally, to bring our tools and facilities to deal with problems of national and international interest. I think that cyber attacks on critical infrastructure in one of those types of problems.

In addition to our laboratories, we also have test sites, large areas where we have rigid power grids, where we have control over the

electromagnetic spectrum, where we can test things to failure. Those facilities are interesting places to tackle tougher questions about control systems, networks, crosstalk, cyber, wireless, and intersections of technologies that can impact the grid. As we think about cyber, we typically draw upon the tools that we have at our disposal, and try and look at it in a broader sense.

Our way of approaching complex problems in our department is through simulation. We extensively virtualize many such problems, and we try to apply a rigorous uncertainty quantification approach, so that the outcomes of these complex predictions are bracketed with uncertainty. Whether it is our nuclear weapons program or any other national security program, there is a fairly deep and rigorous process for simulation, in an attempt to answer complex questions like that.

As far as I know, there is no current model that simulates, in a very detailed manner, something as complex as a nationwide blackout of the USA grid as a result of a cyber attack, which could predict the outcome of such an event with any real accuracy. However, we do try to look at cyber issues by modeling complex enterprises on some of our largest supercomputers, modeling parts of the web to try and understand what kind of failures can percolate through.

As for my greatest concern at present, I am less worried about the kinds of problems that have to do with better hygiene – upgrades, maintaining your system, reporting information, and so on. These are all things that we already do, and many companies and people think about, and working hard on trying to refine it and make it better for today's problems. In the DOE we look at some of the more complex problems, and what worries me are things that can happen to any complex engineered system, such as the electrical grid. That is the sort of problems that everyone knows that eventually will happen, and still always catch you by surprise. These can be subtle interactions between components that are just beyond any individual's grasp, lacking the ability to see the entire complexity of the system. We have to develop tools we can trust to make those kind of inquiries, and I just don't think we are giving the proper attention to that class of problem.

4TH SESSION: CYBER IN MOTION

MATAN SCHARF, STRATEGIC ADVISOR, BLAVATNIK ICRC; CYBER SECURITY SPECIALIST, RESEARCHER AND ENTREPRENEUR

Today I want to discuss the latest trend in cyber security, which is mobility, a subject that is very close to me. This is something that I have been dealing with for the past two years, and I want to share some insights. I always say I wear many hats, one is here in the academia, another one is consultant, among others, but today I want to wear a different kind of hat – a helmet, actually – because we are going on a race, and we will discuss some very interesting things that are happening in the field of mobility and cyber security.

In transportation, for example, I would like to focus on the automotive industry. Over the past hundred years this industry has changed dramatically: from an industry that was based primarily on mechanics, it shifted and migrated into a hybrid mode, where what we perceive as a vehicle is not only mechanical, but also electronic, and that was just the beginning. As the industry progressed in the 1980s and 1990s, what we started seeing is more and more electronic components and software entering the vehicle, but that still wasn't the end. Today we are talking about a true revolution in the field of automotive, and that is where a vehicle – or, at least, what we perceive as a vehicle – is becoming digital, something that we consume as a service. That is very interesting, because that drives the entire industry forward into a completely different way of thinking, and it is very possible that in the future, when we will talk about a vehicle a car or any other form of transportation, we won't be talking about something that is physical. It will have a component that is physical and mechanic, and some of it also electronic, but we will mostly be talking about a service.

This is a very important trend that is happening in the world that we need to understand, which is the migration of the personal computing environment. The entire consumer electronic industry is changing from what it used to be, based as a mainframe and then personal computer and then mobile computing, into vehicles that are increasingly becoming the new foundation or the new infrastructure for personal computing. There are many different players in this field, many originated in Israel – which is quite interesting, considering the fact that Israel is not

renowned for its huge and successful transportation industry. There are many new players coming in, including non-standard competition companies that play in the field of transportation and bring many software-based services – some are cloud services, some are consumer services – into the world of transportation. This is where things get really interesting, because if the industry is based on this type of innovation, the real question: is who is driving this revolution? Who is driving this new industry into these new realms?

The answer lies, of course, in the infrastructure. In this case, infrastructure can be companies like Google, Samsung, LG, Apple, and Blackberry. Blackberry is an amazing company that made phones with secure messaging. People in the USA are very familiar with Blackberry, but in Israel it wasn't the most successful platform, and they were left behind somewhere in the whole Apple and Android war. But when it comes to vehicles, Blackberry is one of the strongest players. They have an operating system called QNX, which is the most popular operating system for vehicle infotainment systems. All these companies are driving forward this revolution, changing the way we are going to perceive what a vehicle is and the way we consume transportation. Of course, every major change always involves a tradeoff, and in this case the tradeoff is very obvious: we are trading functionality, comfort, price, and so on. Which leads me to cyber security.

I think that what I am going to say won't come as a shock to anyone from the cyber security industry, because this has come to be a given truth: anything that is connected, anything that is running software, can be hacked. However, I would like to point out two things – and again, I am focusing on the automotive industry, but that is just one case study, it is true for any type of industry that deals with this sort of things, any IoT industry, basically. There are two flaws in the way that this trend is transpiring, and how that relates to our world of cyber security.

First, I would like to talk about physical access. We are dealing with physical entities – cars, motorcycles, trucks, etc. – and some people have physical access to them. They can be mechanics that connect with a computer to the vehicle, and can do software updates; but it is also the driver. For example, there is an on-board diagnostic (OBD) device that connects to an OBD port in the vehicle, and is mainly used for diagnostics, but one such specific device was used to hack Corvette

cars. It could turn on and off the breaks control, and the other critical systems in the vehicle. In a Tesla vehicle, researchers were able to take apart the console, connect the wires, and be able to ignite the engine without using any kind of key.

Any good hacker will tell you that if you have physical access to the resource, then basically you are not really hacking anything, which bring us to the second flaw I wanted to mention. Radio frequency, or RF, is the underlying technology behind applications that we know as Bluetooth, Wi-Fi, and other forms of wireless communications. There is a tight correlation between the RF technology deployed and the potential for hacking a vehicle through one of its applications. As you can imagine, the more sophisticated the application, the higher the chances are that it will be hacked, and the damage will be higher accordingly, however, there is also a matter of distance, of physical proximity to the vehicle.

Close proximity to the vehicle means being within 5 meters, or 12 feet, from a vehicle, not necessarily to have physical access. In this proximity, we have things like the tire pressure that has an RF antenna, which is able to communicate with the vehicle; we have the smart key applications, mobile devices that can unlock the vehicle with an application, and do other things like turn on the AC. A little further away than that, we still have applications like Bluetooth pairing – anyone can get into a vehicle today, pair their mobile device with the infotainment system, and then they can get your phone calls, share your contacts, and do other things. Bluetooth, as a layer, is secured, but applications that use Bluetooth can still be hacked.

When we go even further from the vehicle, we have Wi-Fi, and then RDS. RDS is the technology that allows the vehicles infotainment system to show you which song is playing on the radio, for example. The range here is 100 meters, and if we take it all the way to fully connected vehicles – i.e. vehicles that have a GSM model that basically turns them into smartphones – you can hack a vehicle from anywhere in the world. This was demonstrated in the very famous Cherokee Jeep hack, by two researchers who managed to connect to the vehicle from anywhere in the USA, from the comfort of their home, or wherever they chose. They could hack the vehicle, control all of the systems, including the steering wheel, including the breaks and everything. This is really the point when we are talking about cyber security in

vehicles: we are talking about a system that was designed to allow for cyber functionalities and features, but not necessarily to accommodate security. And this is really the essence of what cyber is, understanding this tradeoff between functionality and the risk and for ourselves. That means understanding the interface, in this case between a vehicle and its connectivity to the person in the vehicle, and so on.

ESTI PESHIN, DIRECTOR OF THE CYBER PROGRAMS, ISRAELI AEROSPACE INDUSTRIES

I will start by asking: is modern air traffic cyber safe? Just to give you a brief spoiler, I think all of us will agree than the answer is no. We are cyber professionals, we know that everything can be hacked, and everything that can be hacked will eventually be hacked, so the industry must step up in order to prevent the potential damage. I'll skip the landscape, where the fear factor comes into place. We know that there were hacked airports and hijacked airplanes, which caused significant damages, financial and other. We know that the Government Accountability Office (GAO) in the USA claimed that the FAA needs to bring to the table a more comprehensive approach to cyber security. They actually gave alerts about several elements that exist on a plane which, in their opinion, are not sufficiently secure.

Civil aviation needs to step up its game and become more cyber secure. And that industry has a very important role in this context. Looking at the threat landscape, there are physical threats to civil aviation, such as hijacking, onboard tampering, sabotage, and even disruptive passengers; we have seen quite a few of these examples in the past. However, additionally we also have cyber threats, ranging from hacking of ground systems to hacking of supportive systems, such as air traffic management, and finally – hacking the communication of the airplane itself. Some of these elements have been proven.

A very interesting example is "Ghost in the air(Traffic)", a presentation given in 2012 by a very important researcher by the name of Andrei Costin, who basically showed that the next generation of modern air traffic management system, which is IP-based, is hackable, even using very primitive manners. Today it improved a bit, and is not as vulnerable as it used to be, but he showed that you can perform a

very effective DDoS attack, spoof messages, and even claim to be an airplane that you are not.

Air traffic control governs our flights. We need air traffic management to be secure. When we are looking at the operational challenge, the fact of the matter is that when we are looking at the industry we see a huge number of cyber environments that are affecting how we reach our destination, how we get from one place to another, starting from the onboard systems, which today are becoming more and more interconnected; some of them are IP-based. Other systems govern the way through which we reach the flight – the check-in system, passenger listing, baggage control. There are systems that control the plane, such as air traffic management, automatic landing system, and so on. These systems are inter-connected, some of these systems are connected to other external systems, and most of these systems have computer elements. Here I go back to the statement that everything that is software-based has flaws, and eventually can be hacked.

What can we do about it? First, I believe that IT security is not enough, you need to harden the systems to the best extent possible, and this actually means constantly continuing to upgrade them. We have a wonderful cyber industry in Israel, we have emerging technologies that pop up daily and make cyber space more and more secure, but we need to constantly upgrade the security of our systems, because the bad guys are constantly improving their capabilities as well, and we need to run forward in order to stay ahead of the game. However, this is not enough. We need to monitor every possible system and try to detect potential anomalies, because we won't necessarily know that an attack is taking place unless we are able to detect what I would refer to as indicative signals. We need intelligence, intelligence is key; we may not know that we have been attacked, but we may be able to know that there is an intention to attack us, and improve our defenses, close in our ranks, and make sure that we are not attacked.

Finally, and this is a key point, we need to collaborate. Everyone needs to collaborate with everyone – academia with the industry, industry amongst itself, industry with the public sector, governments and governments, various regulators, and in the civil aviation industry, the manufacturers, the various vendors, the integrators, the airports, the airport authorities, the airlines – everyone needs to come together and collaborate in order to create safer air travel. IAI is actually a very

strong believer in collaboration, and for this reason we established, in the beginning of this year, the Israeli Cyber Companies Consortium (ICCC), comprised of seven companies. It was endorsed by the Ministry of Economy, and we are basically marketing end-to-end solutions together, which gives us strength and ability to provide an end-to-end solution, not just a singular solution. And collaboration is the key to a safer cyber space.

When we are looking at airports today we are looking more and more at situational awareness. We are trying to look at an airport from the cyber factor, understanding whether or not it is currently under attack, whether or not it has been under attack, and by doing that we are looking at various IT systems in the airport. This has been done, this is being done, but we are also looking to operational and dedicated systems within the airport. Cyber intelligence can also be harnessed in the interest of airport security. Many of us are going through airports, getting on planes. Using cyber intelligence, we can look at all these passengers, and try to see if we can identify in advance passengers that shouldn't board planes. This is how cyber can be used also in the other direction, not only protecting against cyber attacks, but against potential physical attacks too, finding the bad guys by looking, for example, at their social or cyber profile.

I would also like to briefly discuss the Cyber Air Bill that was introduced in April 2016 in the USA, and is actually a landmark bill. The essence of the bill is, first and foremost, disclosure of information. Airlines, manufacturers, airports, are urged to report any attempted incident and successful incidents against systems on board aircrafts, and against supporting systems – ground support systems or maintenance systems. This will provide a picture of what is happening. Some of us are shouting from podiums around all around the world, saying that civil aviation is insecure, but when you look at the number of reported incidents, not many of those get in the media. The FAA is allowed to share this information as required. Then we have cyber security reequipments as part of the certification process, and finally, there is some emphasis on the management of cyber security risks for consumer devices: all of us board airplanes with our mobile devices, Wi-Fi is widely used at airports, and so on.

Is this enough? No. first it will plug some holes, it is a very important first step, but looking at the entire industry of civil aviation, it needs a

holistic approach for securing air traffic; it needs to incorporate airlines, it needs to incorporate airports, it needs to incorporate manufacturers, as well as all the players that are involved. Eventually, there will be comprehensive cyber legislation related to the civil aviation industry, but in the meantime industries like IAI need to come up with the potential solutions. This is a major part of what we are doing today, we are putting a lot of focus on this, together with our partners, and we keep searching for solutions.

In a matter related to the air-space industry in Israel, and the importance of government incentives, I have been asked if I think that there is an opportunity now for Israel to build an automotive industry, if government funding could play a major role in that.

I think that when we look at the Israeli industry, we see four factors that drive our innovation – and everything here starts with innovation, because this is our strongest point. Number one: where there is a need, there are entrepreneurs willing to fill the need. If there a need for cyber security solutions for the transportation industry – and I think there is definitely such a need for that – we will hear more about it. This is true for the civil aviation industry, but also for the ground transportation industry and for the automotive industry. Number two: Israel is considered a very high quality hub of excellence in terms of innovation, but the technologies need to be brought to the table in order to maintain this reputation, also for the automotive industry. In the civil aviation industry we are seeing and working on some technologies, but this is a process that needs to be funneled in a sense, and government incentives can bring more entrepreneurs into this area.

Finally, there is a question of manpower. When looking at the civil aviation industry, for example, you need two simultaneous proficiencies: you need to understand the language and profession of civil aviation, and what are avionic systems – these are not just regular operational networks – and you need to understand cyber. There are many people who understand cyber in Israel, but not many who understand civil aviation, so if the government wants more entrepreneurs to follow this area of civil aviation and the automotive industry, it has to create a pool of experts in this area. This is driven by two organizations, the military and the academia. Today we have five cyber faculties in

Israel, each specializes in a specific area, and I think the government should try and push more of these young students towards this area.

Finally, I think the most important element is that Israeli entrepreneurs tend to follow the money – if there is a lot of money in this industry, then the solutions will follow. Government incentives can create the initial motivation for these entrepreneurs, but eventually the market will talk, and we will see how the cyber solutions are adapted by the automotive industry, by the ground transportation industry and by civil aviation industry.

ARIK MIMRAN, GENERAL MANAGER, VICE PRESIDENT OF ENGINEERING, QUALCOMM

The car is going through its greatest revolution in more than a century. By 2025, people will no longer need to drive cars in order to get around, and this change is happening step by step. At the first phase, we see alerting systems, like anti-fatigue, which give alerts to drivers upon events. We have internally-facing cameras that monitor the face of the driver, and in case of an emergency, where we see the drivers lose focus, they can prevent accidents. Next, we see driver assistance systems that can self-drive cars in traffic jams and in highways. These self-driving systems actually do better and safer work than humans, and we know that today. In parallel, we have entertainment systems in the car, which make the drive much more enjoyable for the passengers – hopefully, only the passengers.

The collection of all these features is what we call a smart car. This smart car is actually what gives us the opportunity to have a more entertaining driving experience, as well as more productive. But this doesn't stop here, the next thing we are going to see in the future is completely self-driven cars, where cars drive autonomously on the roads, and we, as passengers, just sit there and monitor things. In addition to turning our lives much more productive while driving, it also increases the safety.

The smart car is, by far, the most sophisticated connected consumer product, but it doesn't start from scratch. It comes from technology that we already have in smartphones, which is based on four pillars. The first pillar is connectivity, where we have LTE networks that allow streaming of high resolution videos to within the vehicle. Connectivity

is also used for communicating between different vehicles, and for vehicles to infrastructure messaging. The second pillar is the applications, where we have operating systems, which are in vast use in smartphones, such as android and QNX, now being used in automotive. We also leverage emergency assistance messaging, as well as over-the-air updates. Beside the trivial function of updating applications, over-the-air updates also allow fixing bugs within the car, something that we already have in smartphones.

The third pillar, infotainment, is mainly based on high resolution video engines, as well as graphics, and when we see drivers move the navigation software in high resolution, it is enabled thanks to a very powerful graphic engine. Besides that, passengers can also do productive work as well as watch movies, at least on their rear displays. The fourth and last pillar is machine learning, where image processing is used for analyzing and understanding the surroundings of the vehicle. We allow the main computer of the car to make decisions upon obstacles or pedestrians that are in the surroundings of the car.

Connectivity and smartness in smart cars actually means much more complexity, and we know that hackers that are already hacking PCs and smartphones, so for them a car is simply the next target. One important attribute of the car is that it is constantly connected, which allows hackers to penetrate it from the outside. In fact, researchers were able to demonstrate such hacking – taking over the car horns, cutting the power steering of the car, or even spoofing the rear displays or even the dashboard displays.

The more challenging thing about cars is the fact that they are moving rather than stationary. This by itself is a vulnerability. But not only that – the cars are parked outside, in our parking lots. Usually, we would have our PCs locked either in our homes or at the office, and we would have our mobile phone with us, but cars are left outside, and then any passerby can come and try to hack it.

As cars become smarter, we are calling for a holistic approach to address the automotive security challenge. The first principle is the containment, where we need to start from the core of the car, and then take it through the interfaces and up to the network. By containment, we mean that we have to base it on basic infrastructure, hardware, mechanisms that already exist there, for example secure boot, unique

device key hardware, crypto engines – all those already exist, and we need to make use of this infrastructure in order to provide security in cars. Verified security is another principle. We believe that the security in the car has to be built in layers, in a manner that if one layer is being compromised, then the others are left intact. For example, if we have a denial of service attack over the GPS, it doesn't mean that the attacker can then reach the breaks of the car.

Lastly, we are calling for standardization. We cannot afford a case where every company comes with its own protocol, its own standard, its own way of doing things, it will simply not work. In a car which is comprised of many elements from many partners and players, we need to ensure that all these elements play well together. For this we need to have a standard that defines those. In the Israeli office of Qualcom, we have recently started to work on automotive security, as part of the company's global efforts to address this challenge. We are building and executing upon a road map that we are planning in our office, and we are starting to build the building blocks for making security happen. Besides that, we are making the first steps in standardization, which I already mentioned – taking parts in some of the standard bodies and establishing others. In addition, we leverage the rich ecosystem that we have here in Israel, and always look to partner with start-ups and companies in the field of cyber security, or even better – automotive security, to join us on our beautiful journey.

When asked if I see Qualcom venturing into the realm of being a proper car manufacturer, like Google, Apple, or Samsung my reply is that I don't think we are going to see cars with Qualcom logo anytime soon. In smartphones, for example, Qualcom started from the modem. If 10-15 years ago you asked what Qualcom does, people would tell you that we make modems, but since then Qualcom expanded much within the smartphone. Today's smartphone is much more than a modem, it is a complete SOC with graphics and codecs and RF chips, and everything around that. When it comes to automotive, which is an amazing rich technological environment, we have plenty of room to expand, and I believe that we will see more and more components and technology elements from Qualcom in the future.

CHRIS ROBERTS, CSH AND SENIOR CONSULTANT, SENTINEL GLOBAL

The beauty of humans is that for all that we err, we also have an equal capacity to evolve. it's a really nice statement, and as we talk about the evolution of security and technology, it is a wonderful one to think about. Unfortunately, as a problem with this one, we don't necessarily evolve. We still have to have signs that say don't molest the crocodile, or don't tweet about the fire before you exit the building. As humans, we have a problem when we have to say "don't mess with the wrong edge of a chainsaw".

The challenge, when it comes to security, is: what do we do about it? Thus, the civilized abstract was basically determined, and asked: how can we focus elsewhere? What can we do to make everybody think about things? The reason we decided to do that is because the message wasn't getting through. We would stand here, as we have done many years, in front of audiences, and say, "hey, there are issues with security," and everybody would nod their heads in agreement, and then they would keep on going on with their same life. Our challenge was to understand what can we actually do to make people wake up, and what message should we give them.

We did do four or five years' worth of research, and we are going to talk about why research is important, about why we, as researchers, want to reach out to companies, and about what we have to do as organizations when researcher comes down and says there is a problem with it.

In theory, there are 4 billion people that are going to be connected by 2020, so all the discussions we have about the Internet of Things is rather scary, because there are going to be many people on these systems, with 25 million apps, and we know very well from history that 24.9 million of those apps are not going to be coded correctly, and that security will be an afterthought. That is a very serious issue, and so is the Internet of shiny Things, as we like to put it.

We were wondering how to define our challenge here, and eventually decided to look a little forward, at 2020. At this point, there will be 4 billion connected people. If we take the standard bell curve, this means we have about 15% geeks, 70% regular folks, and the additional 15% is people on LinkedIn, who think that 123456 is a good password. By that time, the population of the USA will be 4.4% of global population, meaning about 26 million geeks, who are about 8% of the entire

population in the USA. When you are talking to audiences about computer security, the chances are, at best, that you are only reaching 8% of that population. This doesn't make us feel so positively about the situation, because we haven't touched the other 92%. Now, the question, or the challenge, is how do we get to them?

The simple answer is: global statistics. There are billions of tons of corn, gallons of ethanol, 1.5 billion cows. Even cows come with RFID tags now. And the list goes on. The concept here is not to focus on the Internet of Things, but how do we look at actually modifying some of the basic elements that the other 92% are working on. We focused on it, and on the food industry, because if you look at the highest 8%, we care about technology and security, but the other 92% don't care about that. Therefore, we decided to research some things and see what we could actually do, and ended up hacking milk. We'll use the UK as an example. We went after milking machines, and did quite a lot of research.

There are many ways to conduct research: Open source intelligence human intelligence, Google research, and various other forms. The ability to gather intelligence on ourselves. Many of us focus inside our own four walls, yet we don't think about what is going on outside, who is going to attack us, who is interested in us. This is a conversation that rarely happens until after we have been breached. We took that same concept, and applied it here, as well.

Once we did our research, we decided to hack milk robots. There are screens showing dairy farms, and even cows inside dairy farms. The wonderful thing about these machines is that not only do they milk the cows, but they also take chemical compositions, they can add chemicals, and can even give antibiotics to the cows. If I have access to this machine, not only can I now kill the cow from antibiotics poisoning, but I can also poison the milk, and I can disguise that. There, now I have messed with your milk. These days, even the livestock is connected, and the ability to move cows virtually is no different than moving aviation. We can have the ability to mess around with the pedometers, the ability to mess around with livestock in general, with the feeding, the nutrients, and everything else in that cycle. So this is how I have taken out your cows. We got your milk, we take the milking machines, we take the pasteurization systems, the IDs, and everything else, too.

When you take a step back and apply the same concepts to yourselves, we have the same issue, you have the same challenges. How many of you take that step back and research yourselves, look at the vulnerabilities you have? How many of you have had researchers talk to you and try to help you understand what your vulnerabilities are? What do we do about it? The problem with the earlier questions, and the challenges I ran into when standing up to the aviation guys saying that they have a problem, is that they go into a defense mode, when we actually need their cooperation. Like all of us who do research, I would rather walk into an industry, tell them that they have a problem and have them listen rather than not. Balance is also important – we want to research, we want to do the right thing, yet for the most part we are met with resistance, which leads us back to the 92%.

Six years ago, we hacked tractors. We managed to drop a smiley face into the assembler code of a set of tractors all around the globe, and it is still there six years later, even after we have told them how to do it. This means that I can now stop you from producing crops. When you put the seed in the ground, if you plant it too deep the system tells you, because you don't know it for yourself. But if you aim to plant it at 2 inches, and the system plants it at 4 inches instead, you don't get food. The same architectural attacks apply to the water supply systems; the SCADA pumps, the PLC controllers, the smart devices that have still got default software running on them, the water treatment plant, the ability to falsify the testing, the ability to inject all sorts of interesting things into this.

How do we do it? We have a TORNADO system for threat intelligence, it is the ability to look outside of the four walls. There is a similar concept in Israel, but only for government-based systems and civilian ones. At the very least, get out there and find out what is on about you as you are developing new tools. What are your database guys doing? What are the network teams doing? Who is talking about you? Do something, rather than waiting until the inevitable happens. The same thing goes for heating and lighting.

At the end of this scenario we have taken the milk, we have killed the cows and the chickens, we have taken all the basics away from you, and all without declaring war, in a non-violent way. Although we did hack numerous things, we haven't even had to go after critical infrastructure too badly. This is what security looks like at this point

in time, it is not a pretty sight. To point something else out, we didn't touch a single one of the Internet of Things shiny toys that we all talk about, let alone advanced persistent threats. When you haven't fixed the basic passwords or the basic controlling architecture in your infrastructure, I don't have to do anything other than to walk in with a spreadsheet that tells me the basics.

Now let's talk about the remaining 8%. In theory, these are the "enlightened bodies", security experts and the audience we have to deal with. The challenge here, again, is communication. We come to organizations with issues and challenges of security, and we get lawyers. We talk to organizations and airlines about aviation security, and when we did it in 2012-2014 we got rebuffed. We talked to the executives who don't care. We bring them our problems, and they sit there and say "we are perfectly fine, the audit that we have says we are fine, we got the check in the box." Unfortunately, this is not the way it really looks.

The CEOs and CFOs, for the most point, really don't care unless they have been breached. The accountants are the same, because security costs money. How do we change this mentality? The lawyers just couldn't care less, they get paid either way. The doctors in the USA, where the healthcare system is a mess, have the most interesting data: not just credits card numbers, but they also have social security numbers, histories, everything, and they can sell the drugs multiple times over. The officials have too much red tape, retailers and bankers spend most of their time trying to convince the auditors that they are secure rather than actually listening to them and fixing the problem.

And then we come to us, the security community as a whole. We are on DEF CON 24 this year; for 24 years, we have been saying, "we have a problem, here is how we demonstrate it," yet nothing has changed. Things have, to some degree, gotten better, yet we are losing more and more data, let alone the fact we are generating more and more data. And for the most part, the other 92% ignore us, and nothing has really changed. What do we do about it? Here is one example: a hacker breaks into a company, he changes your passwords but he leaves you the access to them. He encrypts your data, but gives you the keys to the system. Then he VLANs your network, because you left it as flat as a pancake. And then he tells you what he has done, and he gets the hell out of there, cleaning up after you.

Altruistic hacking. I would love to see this prosecuted – I don't necessarily want to be the one that actually does get prosecuted for it, but it would be fun to do it because arguably it should be done. Could it be done? Easily; should it be done? In our minds, the answer is yes, because logic says that a secure and encrypted system is much more secure than leaving the stuff where we have it these days. Logical argument says we should fix all of these systems. Unfortunately, we are not dealing with logic.

As we are talking about how to break things, we are basically saying "you have problems and we are going to give you a fix," and arguably we should deploy it, and here is why. If you take the human example of a virus and a vaccine, we have taken the best parts of some of the best viruses and Trojans out there. We have taken the best parts of the obfuscation techniques, and some of the best parts of the update and resilience in the architecture, and we have looked at the problem. In this case, we looked at Africa, because we kept on getting attacked by systems over there very frequently. We took the whole idea of the virus, turned it into a vaccine, and then we deployed it.

At the moment, there are 1.2-1.3 million computers in Africa, which are doing nothing more than the job that the person who bought them intended. There are no malicious things there, they are not used for DDoS attacks, they have not been harvested for any data – they are simply sitting there, running a vaccine. They probably still have antiviruses, and every now and again somebody thinks to patch them. Not that those are much use either.

We didn't ask anybody to do this. Nothing was harmed or taken or stolen, but they are now no longer being used for abuse. We may have bent a few rules in the process, sorry. So, yes, we hacked into 1.2 million computers, but there are no evil Overlord intentions, there are no backdoors in the code, there is no masterplan to take over the world, there is simply the desire to see change; to see systems get better without having to go through the bureaucracy of getting them fixed.

There are so many embedded systems out there that need fixing, and there are so many bureaucratical organizations that don't want to fix them, or don't believe they should be fixed. I personally say: "fix them first and argue about it afterwards". Stop saying how "we can't do things", and start saying "how do we solve it?" we have to change

the approach, we have to say who is dealing with us, who is working with it, and where the focus is. Stop standing up here and say that over the next years, blue blinky lights are going to fix everything, because they're not. Instead, start actually cooperating, because from my standpoint, I really want to go after the eastern sea board in the USA, and when I do that, I am going to be sending messages to the space station, which is simply going to blink "fixed by 127.0.0.1".

Lastly, I was asked about my membership in Hackers for Charity, and about the ability to reconcile the desire to create a significant impact with the associated risk involved om illegal actions. I think you can take the ultraistic hacking approach and apply it in certain circumstances. Hacking into a company and trying to fix their problems is, unfortunately, likely to cause more issues, because you try and repair the healthcare of machines that can't be scanned, because the vendor says that they are too unstable, at which point you are going to break something. But when you come to look at PLC controllers or skater systems or anything else where there are obviously flaws and issues, or even the stuff that we did in Africa and in a few other places, where nobody is helping, nobody is fixing, nobody is solving – yet those systems are being used every day to run DDoS attacks, the people's data is being harvested on a daily basis.

At some point in time, you either take a step back and accept that, meaning I am done dealing with it, or you say "I just want to fix it." It is that desire to fix something, and you deal with the consequences. There is no easy solution, but the problem that is standing here and doing nothing isn't the solution either, and we still lose so much data. It is such an industry stealing data from us, therefore what can we do about it? After more than 20 years of arguing to fix the problem, at some point you just take the humans out of the equation and fix the technology.

SECOND ASSEMBLY

OPENING PLENARY

MAJ. GEN. HERZI HALEVI, CHIEF OF DEFENSE INTELLIGENCE, IDF

I would like to talk about cyber and security, cyber and army, and cyber and intelligence. But before that, I wish to open with something that is not entirely related to cyber, in order to give the context to what is happening around us. For nearly sixty years Israel had an army that was designed to fight against countries, but this is changing. Tomorrow it may be an entirely different picture. This story changes all the time, the entities may be smaller, but they are in constant movement. They divide and reconnect, and cyber, as a flexible and quick dimension, is incredibly suitable for action in this world. The world of warfare has changed, we prepare ourselves to face organizations, cyber changes the strategy, the systemic planning, and also the tactics, and I believe that we are only in the beginning of the path to understand all of those things.

I would like to mention three revolutions that have been taking place for quite a few years, and are currently combining to form a very significant accumulative impact. The first one is the information revolution. For a long time, the challenge is no longer to bring in the information, but to filter it, organize it, extract it. The second revolution is the digital revolution. I think of how, as a company commander, I was talking to a fighter pilot, and how we could talk about a certain formation, where I wanted to explain to him where my problem was. How complicated it was to tell him, "look at that tree and at the blue shades". Today we are fighting in a world that is anchored in digitation, pixels, in X and Y and Z, which makes it very easy to talk about the same point. The third revolution is the network revolution; today we have the capability of

making information and knowledge accessible and bring them pretty quickly to almost anywhere. We haven't completed doing everything in all of those revolutions, but they are very significant. Those three revolutions caused a change in what is perhaps the most important principle of war: concentrating the effort.

In the classic age, when we talked about concentrating efforts, the test was how many vehicles and people you could squeeze into a single square kilometer. Today, in the digital age, the network age, concentrating efforts is how many people you can put in the network. They can be very far away from each other, even in a different time zone, you can even make them act for you so that in a certain point in time, something you wanted to happen – will happen. And this really changes wars.

What am I going to talk about? I'll talk about Cyber, whether or not it is a warfare medium, and if so – what are its characteristics, and its impacts on the world of warfare? I will talk about the connection between cyber and intelligence, which is a very important part of the cyber world, in my opinion; about the power structure in cyber, and the various component in this dimension, of collection, protection, and attack.

The first question was, is cyber really a medium of warfare? To discuss that, I would like to refer to the three classic dimensions of warfare – land, sea, and air, because cyber is different. What is so unique about it? Out of these four dimensions, cyber is artificial, it was made by man, it is defined by man – unlike the land, sea, and air. This is something that is man-made, and we are trying to examine how to deal with it, so the understanding of the people who operate it is very important, and it is akin to understanding the laws of physics that exist in the land, sea, and air, to know how to operate correctly in this dimension.

Cyber is actually a dimension, but a different dimension than the rest. It is a dimension that connects and intermediates between other dimensions. If I have airpower and my enemy doesn't have airpower, I can use this airpower to attack the enemy. If I have cybernetic power and my enemy doesn't have it, there isn't much I can do with that power, meaning that it's a dimension that must exist on both sides to be able to use it. We examine where we are on the scale between 0 and 100 on fulfilling the potential of cyber in warfare, and here I would

like to make a very short comparison to the development of the air dimension, which was the last one to be developed, in the beginning of the last century. The Wright brothers flew the first airplane in 1903, and in 1915 something very significant happens – someone managed to coordinate a suspension coming down through the airplane's propeller, which is an important thing. It's not good to hurt the propeller when you're in the air.

In World War I the airpower was more of a spice, or added value. We can't say that this was what won this war, it participated and developed within it; however, in World War II, about 30 years later, the airpower was the force that won battles. What happened in the time between those two wars? There is understanding the potential and there is realizing it. We are in the cyber world once we have already begun to understand the immense potential this dimension has, which is quite similar to the period nearing the end of World War I. We still don't fully understand the potential, and certainly not how to realize it. When you look at the purpose, in land we want to conquer, and in air and sea we want to prevent movement of others, and make our own freedom of movement, which will allow us to attack. What do we want, what is the purpose in cyber? In cyber we want to hurt by manipulating, for the worse, the products of those three revolutions I mentioned earlier: information, digitation and networks.

If an army builds its strength and trains in a certain manner, and you manage to take a substantial part of its abilities in the beginning of the war, it is a very significant achievement in the battlefield, it is the equivalent of many kinetic efforts and much work in the battlefield. Where can we get a clear picture on both the potential and its realization? We get it in the world of intelligence gathering; here we have already accumulated a very good mileage, we understand the potential. Some highly significant parts of today's intelligence gathering come through cyber, or are at least tangent to cyber, and this trend is very likely to continue getting stronger. In contrast, we are still trying to figure out the other two components in cyber – attack and defense. We already know the attack aspect, we have tried it, but we still have a long journey before we understand its potential; and defense is like a helmet for bicycle – it's not good to go out on the road without it, and it better be good, too.

When it comes to the development of this dimension, the period of ignorance is over. In the first years, we enjoyed the low-hanging fruit that were easily reached, but today the world is learning. Everything is getting harder, and when we look at examples published in the media – and I'm not saying this as an intelligence statement – about attacks in Estonia, Georgia, and recently in Ukraine, the electric systems; the Snowden affair that allowed a peek into the cyber capabilities of superpowers; about two incidents in North Korea; Sony's anecdotal incident; and a fairly recent incident, from February 2016, where $81M were stolen from the central bank of Bangladesh, probably through SWIFT access. There are very interesting events, and the world is learning and defining the rules. We are a part of this race, intelligence provides a very significant added value, and the intelligence superiority I am about to mention allows managing the risks of operating in this dimension.

How does cyber affect the world of warfare? I believe that cyber changes many of the concepts that allow us to realize the fighting. First of all, the definitions of enemies and friends. We are used to simple, binary definitions, but today the range of possibilities is much greater: an enemy, a rival, a friend, a partner, there are protection companies, there are hackers' militias, ideological armies like Anonymous; but there are also second degree changes – it isn't only the range of entities that can exist, but also, the same entity can exist in two different hats. Take the company that protects you – you can meet that same company on the other side, on the side of the enemy against which you operate, and there it can be your rival, not to mention even your enemy. This world here is more complex; definitions of boundaries, spaces, what constitutes "enemy territory" in the cyber dimension, those are all problematic definitions, which are certainly very different from the "ground" world.

When we look at concepts of time and space in Newtonian spaces, they have a dramatic impact – this is what every officer learns in his first positions. Know how much time it takes you to bring a force from point A to point B. The firepower and maneuvering are blocked due to questions of time and space, and intelligence gathering is also blocked in physics. You're blocked in the lookout, the mid-range – the antenna reception range – but cyber bends these things. Cyber shrinks space and time and distance in the manner that through the

network, you reach a camera that can be at the intersection of two streets in London, a city with many cameras, and bend the physics, and get the communication from there almost in real-time. The same goes for antennas.

There is a wonder in cyber, it allows us to move back in time, intelligence-wise. We are used to idioms like "no use in crying over spilled milk", or "whatever happened, happened", but in cyber it's different. Suddenly you get a database filled with information from three years ago, and you go back in time, and from that point you start developing and crosschecking that database with other things, you get to the present and you don't stop there – you continue to go forward, into the future. And we discover that in cyber you can actually operate back and forth in time, and benefit from intelligence that can manipulate things that have already been done a long time ago.

The operation is covert, it has existed since the dawn of warfare, in the Bible stories, the spies story; but it seems as though these thousands of years have only been some sort of a promo, and were only waiting for the real thing in the covert world – cyber. Cyber has something that fits like a glove to the hand of covert operations. You can do things there under identities that are difficult to track, you can operate remotely. The invisible boy Danny Dinn, from the Israeli youth book series, didn't know this patent, and perhaps this series can now be rewritten from scratch.

And so, we find ourselves at the IDF using cyber in the campaign between wars, which we call the CBW, a concept that the IDF has been dealing with for about a decade. The purpose of this campaign is to keep the enemy deterred, to restrain their gathering of forces, and to prepare us for the next war, all without entering another war. Cyber is a player with substantially central potential.

I would like to talk about amassing power in cyber. Cyber security specialists are not a crowd of an equal distribution to that of the general population, but if I showed you two photos, of an F-35 fighter and a server farm, and asked you which photo was more beautiful or attractive, most people in the world would point at the F-35, of course. We are facing a challenge when we come to the IDF and trying to convince them to give us budget for power structure. It is very hard to compete against this beautiful fighter, although it is still

in its first steps. In contrast, a room filled with servers doesn't seem as attractive – why do I have to pay so much for this thing?

In addition, there is a very significant difference in the power amassment process, long strengthening and equipping processes that take five to ten years. The Air Force gets a new fighter plane every decade, and they are very, very different from each other. In cyber, we build our power in a telescopic manner, with modular options for changes, adjustments, we build the basic capabilities, and then quickly develop the end-capabilities in short ranges of time.

What is the purpose of all this? The purpose is to reach superiority in cyber. First of all, superiority is a relative term, it is always compared to another, but it is also freedom of action in this dimension, both strategic and operative. The condition for superiority in cyber is superiority in intelligence. But here is the important thing – superiority in intelligence requires superiority in cyber, and vice versa, meaning that there is a symbiotic relationship between these two concepts, which I will elaborate on shortly.

This "superiority" is a vague concept, so what are its components? Super-calculation abilities, very important, technological infrastructure that allows research, enables creation of high-level instruments, and experimentation laboratories that allow testing all of those before going out on the battlefield; data-reading capabilities, informatics, covert culture and intelligence way of thinking, because if you're not stealthy you will probably lose much of your power; and, of course, very high level of people, which is, perhaps, the most important condition for superiority in cyber.

I would like to say a few things about gathering, defense and attack, the components of the fighting dimension in cyber. In the beginning, it seemed that they were on the same plane, but today it is clear to us that gathering is a broad base required to realize the rest, and defense and attack can follow it.

First I want to say a few words about gathering. Nowadays, communication is not a product in short supply, and in many ways, the challenge moved from the ability to bring in the information to the ability to filter and extract it. The signal-to-noise ratio that we encounter is much more complex, there is much more noise. This, obviously, challenges our information gathering capabilities. When we look at our challenge,

we see today the cyber capabilities of superpowers in the hands of individuals, tools that used to be owned only by superpowers or countries who received them from superpowers are in the possession of every activist of the Islamic State that operates, as we define it, in sort of telecommuting nomadism. They possess a very strong encryption, which changes in very high frequency.

In the past, our gathering targets were the enemy's military communication system, or the phone line of a leader whose state of mind we wished to understand, but today's cyber signature is much more extensive. Phones, mobile phones, databases, social networks, car computers, biometric identification, and the list goes on, of course. What is the result of all these things? I can tell you that "one kilogram" of intelligence costs today much more than it did ten years ago; its price has increased because technology is more expensive, it has increased because the technology changes much more rapidly than before, and the expiration time of products has grown shorter.

To end the discussion about gathering, I would like to say a few words about social networks. Wael Ghonim said, referring the Arab Spring: "it revealed the greatest potential of social media, but it also revealed its greatest disadvantages. That same tool that was used to unite us to throw down dictators, ended up as the thing that separates us from each other." We are talking about how to conduct a research in the social networks. There is much information we can gather there; we are only at the beginning of the journey with this thing, and it seems very, very important.

We ask ourselves, can we spread an alert for war or terror acts via social networks? We probably can, but it isn't a system we understand in full, all the way, and we always look for improvements. We also want to make an impact on the social networks, meaning that there is a question which many countries face these days: is it the right thing to have cyber and awareness battalions that would bring in new ideas into the network – sometimes positive, sometimes ideas that oppose a different ideology, for example, to deal with the challenge of Jihad worldwide.

Looking at this quote, the person who said it is even more interesting than what he said there. Wael Ghonim was the man who created the Facebook page in Tahrir Square in Egypt, you can say that he is the

person who brought the regime change in Egypt. And he has a very profound insight, which I think we will learn from it and grow from it – the social networks are very good at dissembling things, and it is very hard to reassemble them again using those networks. And speaking of dissembling and assembling, this is a good time to talk about defense and about resilience of things.

You cannot be a significant player in the cyber dimension without good defense capabilities. The key to defense is intelligence, and the best ROI in defense is knowing your enemy – both their capabilities and their intentions. From here, we have two directives: the first – everything fixed can be hacked. This is a directive that also exists in the physical world; the line of contact, the line of defense, will forever be breached. But there is something else here, too. When I was a division commander in the border with Lebanon, and I wanted to implement variable defense, it was extremely difficult. You cannot move your physical infrastructure every day. This is no simple feat even in the cybernetic world, but there is still more freedom of action here. Everything fixed can be hacked, and therefore we need variable defense, and we have to invest greatly in smart monitoring, secret monitoring of the kind that float anomalies, and allows to spot the areas where more profound research should be conducted.

Today we are facing a dilemma concerning how to structure ourselves. On the one hand, we want segregation; where we, the security entities of Israel, operate, we want to operate in a segregated manner, so that no one would be able to penetrate our networks. On the other hand, we want worldwide network connectivity, we want an intelligence researcher that handles classified materials to be able to access databases all over the world, or use an open source code, or be able to update a program very quickly. There is a substantial dilemma here, and we don't yet know the solution for it, but I think that we are on the final stretch – perhaps a very long stretch – of the segregated systems.

We are looking for a "dry swimmer", one who can jump into water and come out dry. If you've ever seen a duck coming out of a lake, you know it comes out dry. We are looking for the equivalent of the material spread on the duck for our networks, to allow us to be inside the network, but in a sort of vault that will allow us very good interaction, while maintaining protection in a very high standard.

Coming from this point, a few words about attacks. The entry ticket to the world of attack is sufficient defense capabilities versus your opponent. When one comes to ask what you wish to do in attack, many times, because technologists mainly like gadgets and development of capabilities, we ask what can be done according to the toolbox, which is a failure. We use the phrase "someone that has butter on his head, better keep away from the sun". In this dilemma, it is better to be vulnerable but advancing in the field than invulnerable but lacking in capabilities, and the balance between the components of this dimension – defense, attack, and gathering – is the key to enjoying this dimension and remain protected at the same time.

Here are some facts about intelligence and cyber. In the physical dimensions, science provides the explanation for their behavior. In contrast, in cyber, since it is an artificial dimension, it requires dealing with intelligence to understand the behavior of this dimension. There are no fixed rules, but a constantly-changing intelligence flow, which has to be reexamined all the time. The power structure is not generic, it has to be directed exactly at what the enemy is preparing, and it requires incessant interaction about the enemy's capabilities and intentions. A bomb dropped from an airplane is not stealthy, once it leaves the wings of the airplane it will achieve its goal when it hits the target. In contrast, if the enemy knows that a malware is going to attack them through the cyber dimension, there is a good chance that they will know how to deal with it; therefore, in cyber, a stealthy attack is of the highest importance.

To conclude the story of intelligence and cyber, knowing your enemy, the manner of exerting your forces and the secrecy connect the cyber very strongly to the intelligence world. How to get organized in cyber? Israel is becoming organized in this matter. We have heads of entities that handle this topic, and I think that the IDF and the rest of the security entities must integrate with this national process of organization. We are a small country, we have no excess of high-quality people for this thing, we cannot have duplicate systems, and we have to know how to work in very clear boundaries and assist each other in crisis situations.

In the IDF, cyber has been already defined as a warfare dimension, and the Chief of General Staff has decided, about a year ago, to establish a military cyber branch, and in the next few months we will discuss matters such as how this branch should be established, where it would

be placed, and how exactly it would function. In my opinion there is no battle here about power or influence, but mainly a mystery. How to find a solution that benefits the wonderful synergy, which is one of the strong points we have, of cyber with intelligence.

When I mentioned superiority in cyber, I declared that the most important component was the people. I think that in the next five years we have to make a great change in the world of people in cyber. The Israeli security forces, that usually keeps very much to itself, needs to open up. I think that in the next few years we will have to see many more joint ventures of the cyber security forces with the industry and the academia. These things are not easy to fulfill, of course, they will require new rules – how to prevent conflict of interests, how to price, how to keep secrets safe – but I think that if we want to continue leading, and maintain cyber as a cutting-edge matter, we will have to develop here a new and different capability of working with people.

The intelligence Directorate in the IDF contributes much to schools in Israel, and develops people who are of good use to us in the Intelligence Directorate, but also contribute a great deal to the Israeli economy in the field of cyber.

I would like to conclude with six short insights. Cyber is a special dimension of warfare, it connects between bits and people. The world of warfare is changing, wars are becoming more technological, and if you ask me what wars are going to look like in the near future, I believe that in the next decade the kinetics will continue to lead, but the share of cyber in the war will increase more and more. It is better to be advanced and vulnerable than to stay behind in the field, but being a leader requires a very good balance between protection, gathering, and attack.

A short while ago Google's CEO, Eric Schmidt, visited Israel, and I heard him say, in one of the lectures he gave, that Google wants to make the entire world smarter, but that he thinks that we here, in Israel, want to keep everyone around us a little less smart. And yes, it is very important to us to maintain this advantage. To me, the combination of intelligence and cyber is a very important point in this lecture. Intelligence as a foundation for superiority and operations in cyber, and a profound understanding that intelligence doesn't contain cyber and cyber doesn't contain intelligence, but the relationship and

affinity between them is very important, and it is unprecedented in comparison with the other dimensions.

Superiority in intelligence is one of the foundations in Israel's security strategy. Today this superiority is achieved, in many aspects, by correct use of cyber, and therefore it is extremely important that we find a solution to develop cyber in Israel in a way that will conserve this.

Lastly, Israel has a substantial technological advantage, and it is unnatural that it would remain that way. Countries that surround us, mainly Iran, become more and more technologically advanced. What is the key in conserving this advantage? Proper education, a technological and scientific society, and proper organizational moves. If we organize ourselves the wrong way, we may give our enemies the time-out they need to catch up with us.

The Intelligence Directorate in the IDF has an extensive tradition of achievements in the field of cyber, and I hope to see this tradition spread into the industry, the academia, as well as partners all over the world.

YORAM COHEN, FORMER DIRECTOR OF THE ISA (ISRAELI SECURITY AGENCY)

Fourteen years ago, the ISA received a mandate from the government of Israel to protect and defend Israel's critical infrastructure, such as utilities and railroads, from any and all attacks. Since then, several attempts were made to breach Israel's cyber defense and destruct our most critical infrastructure. Although our enemies are skilled and persistent, not a single attack has succeeded, in particular in disrupting any of our critical infrastructure. I am here to share with you some insights into how the ISA has fended off some of the world's most sophisticated cyber attacks.

The ISA is cornerstone of the Israeli national cyber efforts, leading the country and synergizing all aspects of cyber security. Over the years, we have developed unique strategic concepts, which are based around proactively defending both online and offline. We don't rely only on our cyber arsenal, powerful as it might be, but approach the threat integrally. The entire intelligence arsenal is used to maintain cyber security. ISA cyber officials extensively rely on signal intelligence,

human intelligence, data mining, and even boots on the ground, in the form of tactical operations, in order to fight the cyber war on the intelligence battlefield.

This concept does not come easily, and it is the result of a decade's worth of extensive capability building and experience. How did we do it? The first step in building an effective cyber ecosystem is understanding the area in which cyber threat plays a role. The basic tenets of the ISA's mandate include early disruption of terror, as well as counter espionage, preventing exposure of state secret, and foiling threats of subversion. This are traditional kinetic threats which, unsurprisingly, are all found in cyber as well. They are called cybernetic threats.

There are three types of primary threats in the cybernetic arena: (1) CNA, computer network attacks; (2) CNE, computer network exploitation; and (3) CNI, computer network influence. CNI is the new and rising phenomenon, which manipulates the public opinion and interest by using cyber tools and methods. Ours is an open democratic society, which rely largely on the web to ingest information and form opinions, and whomever is able to control the flow of information according to their particular interest has ability to determine public opinion, and even set agendas.

Cybernetic threat characteristics pose a grave danger in all those areas. The threat characteristics are: (1) the number and variety of adversaries that we are encounter, such as nation-states and terror organizations; (2) a lack of operational depth from which to maneuver, due to the short waiting period, before an act is carried out; (3) the soft belly which the internet presents to the bad guy – it only takes one innocent mistake, and they are in. This, of course, is a double-edged sword for bad guys, because it gives us great opportunities as well; (4) over the past year we have witnessed the rise in threat intensity for long insider actions which have the potential to cause great danger. I would also like to burst the myth of retributions. It is not a problem to find out who is behind the attack – it may take a little while, but in the end, we always know.

You are probably asking yourselves, what does the ISA do to keep the net clean? In 2011, at the beginning of my term as ISA director, we established the cyber command based on an integrative concept. The command uses all the capabilities that the ISA brings to bear as

an intelligence organization. We have intelligence, cyber analysis, operations, and technological personnel working in conjunction with IT, and guarding a massive amount of human and signal intelligence, while using a variety of methods. The cyber command is not only responsible for defense, but plays a central role in the offensive capabilities of our organization.

What the ISA needed was not just to evolve to the next stage. We needed a revolution; we had to get proactive and quick, because the best defense is offense. We needed to put ourselves in the attacker's territory, sleeping in his back yard, in order to preemptively foil any threat. We integrated the defensive and the offensive units under one commander, on the premise that our offensive capabilities, which have proven themselves time and time again, can be applied to the world of cyber, and break knowledge barriers. This integrational concept is unique and has generated much interest in the international intelligence community.

The second step of the process was the establishment of a cyber operation center that works 24/7, in which all our sister services are represented. We all understood that its impossible to succeed alone, and we welcome and appreciate the assistance of cooperation which was received from all the Israeli intelligence community. This cyber operation center has decision-making authority as well, and a wide arsenal of tools in order to carry out operations against any identified national cyber threat. Our national cyber operation center, which operates under the umbrella authority of the ISA, has foiled several major attacks on Israeli targets due to the unified authority and power.

Our daily dilemma remains the same – whatever we are dealing with, kinetic or cybernetic threats when foiling the adversary, you need to make sure that you don't tip your hand too soon; not to lose valuable intelligence, but not to wait too long, and not allow the attacker to succeed. All of our adversaries used the same basic logic, and worked towards the same objectives: they want to spy, steal data, expose secrets, and terrorize the target. They try to do this kinetically, using traditional methods, but they can also do this cybernetically. If there is a weak spot in the synergy between cyber and traditional efforts, the attackers will be sure to expose it. That is why the integrative approach under one commander and one responsibility is so important.

Did you know that in 2005 only one in every twenty ISA employees was in a technological position? Today, the ratio is one to every six employees, and shrinking daily. The change in technological orientation, which is accorded, is a key factor of changing the organization's mindset. We took a good look at the existent HR norms in the organization in order to harness the incredible technological power that is represented in Israeli society, by understanding that we are dealing with different typeset and traditional recruits represented. We offer a position at the top of the Israeli cyber community, different than the rest of the ISA, and different than existing opportunities in the world of technology.

Within the frameworks of the ISA operational needs and mandate, we were able to offer hackers a legal license to deal with identifying cyber threats to Israel's national security. This allows and drives the top percent of Israel's cyber minds to try an adventure alongside a deep feeling of patriotism, something they cannot obtain in the private sector, and allowed us to recruit and preserve the best of the best.

In conclusion, I would like to say that Cyber threats are not an act of God or a phenomenon in which computers commit acts of cyber warfare and crimes. The real threat is caused by real human beings and those who send them, and they must be held fully responsible for their actions. The only way to fight these threats is for the intelligence agencies to commission and build relative and effective operational tactical capabilities, which will allow them to properly fight the battle on the field in which it is being fought – a dynamic and evolutionary era of modern cyber warfare.

No nation needs to stand alone in this fight. I am a firm believer that united we stand and divided we fall. In the face of this global threat, the international community must pull together, and establish regulation norms in order to effectively deal with this threat and safeguard our society.

BUKY CARMELI, HEAD OF THE NATIONAL CYBER SECURITY AUTHORITY, PMO, ISRAEL

I am very excited to present today the National Cyber Security Authority (NCSA), and I would like to present it through the following question: what makes the difference between securing organizations versus defending a nation? I would like to begin with our mission statement at

the NCSA. As you may probably know, on February 2015 the government of Israel approved the process of establishing and founding the NCSA, the major mission of which is to direct and to manage all the cyber defense efforts in the Israeli civilian cyber space, while, of course, following civil rights, securing privacy and propriety information. Those three keywords, civilian cyber space, are very important. I would like to explain what do we mean when we say civilian cyber space.

The Israeli cyber space includes processes and digital data that belong to Israeli corporations, companies, entities, and individuals. It also includes the IDF, the agencies, police, and the defense industry, which is guided by the minister of defense. We call them "special entities". This space also includes the critical infrastructure – In Israel, we don't define specific sectors as critical infrastructure, but instead we have special companies that we don't regulate, we just pinpoint those companies, and we have a special law that defines how to guide and instruct those companies. But we also have important sectors: governmental affiliates, ministries, the business sector, and of course, the individuals.

If you take out the special entities, then you get what we call the scope of the NCSA responsibility. It begins with a critical infrastructure companies, continues with the business, private, and public sectors, and ends with individuals. This is a huge space, larger and wider than any other space domain in Israel. The next question is: what do we mean by saying that we defend that space?

The first step when you go out and try to defend this space is to build a well-defined defense model, and we have one – a multi-layered defense model. We start with the robustness layer, which means using the best of great technology products, experts, intelligence – use everything you can do the best you can get. But this is not enough. Next is the resilience layer, which means, in two words: be smart. Don't just use technology, use other tricks like traps, honey pots, redirection technologies, deception; do whatever you do or whatever you can in order to mislead your attackers, your enemies.

In our model, we discern etween situation where organizations are under attack and a situation where organizations are not under attack. the switch from not being under attack into a situation when you are under attack is based on intelligence sharing of information with

colleagues or other countries, technological indication, etc. However, once you are under attack, we have a special model how to deal with it – how to take organization from the attack state back into normal state. This is what we call IMM, the Incident Management Model. Right now we are working on what we call CMM, Campaign Management Model, which means what happens if a certain attack goes not just into a single organization, but appears in several organizations, what if an attack has more than one variation, and so on. In addition, we have what we call the concept of operation: how to take all the departments in the NCSA and turn it into an operational entity. But, once again, this is not enough; you need to do more in order to defend your country.

The second step is to develop operational response capabilities. We use dedicated as well as commercial technologies, we use experts, we use concepts, and this is the first time I have the privilege to present the CERT we built, our Cyber Emergency Response Team. It is a well-known entity, located in Beer Sheva. We believe that by the end of 2016 it will be operational, and this is another key to define our operation response capabilities.

Once you have a good defense model, as well as some capabilities to respond, how do you get access to the market? You need to get access. And here comes the third step. We developed several types of access: direct access to infrastructure companies, and indirect access through sectorial regulators. We are currently mapping critical processes, to find companies that are not necessarily critical, but contribute to the critical process, and so we need to guide them. We built governmental cyber defense units, and we do more in order to get access to the market.

Intelligence is also very important. We discern between open source intelligence and other kinds of intelligence. Using open source intelligence, we develop our own production zone, which is based on WEBINT, industry cooperation with large companies all over the world, virtual entities, and Darknet access. The other kinds of intelligence are the Israeli agencies. We distinguish between information or intelligence about attacks, penetration and infection technologies on one hand, and information about attackers on the other hand. We understand that a specific attack may appear from different places, regardless of who the attacker is, and so we make the distinction and focus on attacks and technologies of attack. Also, of course, we build what we

call situation rooms and control room, whose purpose is to create an aggregated picture of what is happening in the venues and take decisions.

Synergy with other agencies is also very important. We welcome any synergy with all agencies in Israel. Only recently we finished the process of signing agreements with all agencies and the IDF. It is very important for us, because we understand that in order to create a complete defense model, we need to work with the other agencies. This is why we established what we call a defense forum, which is led by the authority, but the all other agencies take part in it too.

One sensitive point that everyone is aware of is hiring good people in order to make it all happen. Here I would like to say something from my past experience in business. I talk to my friends from the industry quite a lot, both those in Israel and abroad, and they all complain about their salaries, and about the competition between the business world and the industry versus governmental salaries. Here is my opinion: first of all, don't even try to compete. There is no chance to compete with the high salaries, definitely not with the extremely high salary, not with the stock option plans (SOP), the bonuses, the fancy environment and so on. What you are not allowed to do is to provide them a below-minimum salary and compensation plan, but what you can do is give them the average level, perhaps even above it. At the same time, you can also provide them challenge and attraction. In cyber, the Israeli domain is something that many Israeli people appreciate, and are willing to join us.

Another small word that you can use in order to attract people is leadership. We have experienced managers, people who have already worked for the industry or other agencies in the government, and these people they bring experience, they bring their own charisma and leadership in order to attract people and build a team. I know that the salaries in the government sector are not as high as they are in the industry, but the combination of fair conditions, the hype of cyber, and leadership, is the key. You will not be able to hire everyone all the time for any position, but it does give you a competitive edge.

Now we are getting to legal support. This is an issue we are working on right now, what we call "cyber law", which, at the end of the day, is supposed to regulate or empower the authority to fulfill its mission.

We are an authority, we are not another intelligence agency, this is very important to understand. I explain to some of my colleagues overseas that in Israel, in Hebrew, there is a big difference between the words authority and agency. We do and will do what we have to do in consent and acknowledgments, not in the background. This brings to the table the defenders' dilemma, how to find the working point between defending the industry, let the industry work, and still maintaining peoples' civil rights.

The eighth step is what we call collaboration and cooperation with other countries. The virtual world is not a boundaries world. An attack that starts in one country may target another one. Moreover, attacks may be replicated or simply distributed over global network communication. This is why we believe in collaboration with other countries, and welcome every collaboration with every country that we can cooperate with. We are talking about CERT-to-CERT, which, in a way, is the easiest way, but also about sharing of information, alerts, information about attacks, legal, ideas, technologies – whatever we can do in order to make us more protected, and contribute to the other side's protection as well. Another thing we are talking about here is workgroups – we believe in workgroups and round tables as a good approach, a good platform to exchange ideas and information.

The ninth step, the last one, is regulation. In Israel, we identified four areas where regulation really contributes to security. One is what we call security professions; we define several professions in security, and we are about to regulate them and enable people be certified. The second is professional services, something that is currently under progress. When you hire a company to make a pentest to your network, you know that you hired the right company for the job. We are currently working on regulation related to products and technologies, and there is a background work about what we call certified providers, which relates mainly to supply chains.

We believe that if you go all this way and take all these steps, you can create your own well-defined model, instructing how to defend your system, from the robustness layer and all the way up to a campaign management model. If you create your operational capability and you do all of the things I mentioned earlier, then at the end of the day you create what we call national defense system.

To conclude, defending a nation and securing organizations are two different challenges. While securing organizations requires you to develop the robustness, the resilience, and the incident management model, in national security the building blocks are much wider. Over the past four years the Israeli Bureau of Cyber, led by Doctor Evyatar Metanya, initiated many actions and operations in order to create those building blocks. Now, the job of the NCSA is to take responsibility, take these initiations, and make or create a solid, well-established operation, in order to secure the country and the cyber space. We are here in order to make sure that every person and every business in Israel will be able to use the cyber space with no fear. That's what we do, and that's why we do what we do.

1ST SESSION: STABILITY IN THE INTERNATIONAL CYBER DOMAIN

DAVID KOH TEE HIAN, CHIEF EXECUTIVE, CYBER SECURITY AGENCY, PRIME MINISTER'S OFFICE; DEPUTY SECRETARY (TECHNOLOGY & SPECIAL PROJECTS), MINISTRY OF DEFENSE, SINGAPORE

I am here to talk about stability in the international cyber domain. In my view, the meaning of stability is to be a resilient and shock-resistant system that has the ability to mitigate and recover quickly from cyber attacks. The Singapore government recently tried to implement this, and announced, just two weeks ago, that we will be separating internet surfing. It is part of a concrete step to increase the resilience of our government systems. The policy to separate internet surfing means that government network computers will no longer have direct, unvetted access to the internet; principally, no more surfing or downloading. You can still send and receive emails to and from citizens, and you can still connect to our government network, and our offices can still connect to the government networks from outside the office through a VPN. However, as expected, this became the talk of the town as the media took this story all around the world.

The Singapore government offices will still have access to the internet, just not using network computers, and for very good reasons. Singapore's cyber domain is under constant threat; we are a prime

target for cyber criminals, activists, and even state-actors. As public servants, we have a duty and responsibility to protect government systems as well as citizens' data. It is crucial that we prevent breaches and disrupt what is known as the "cyber kill-chain" to raise out cyber defenses. Internet surfing separation will significantly reduce the attack surface, and prevent attackers from exploiting our systems.

The purpose of our government's move is not to restrict public sector access to the internet, but rather to segregate, and secure our e-mail systems from other activities that we conduct online, such as browsing or transactions. Some reports in the media say that the government e-services would be disrupted, which is, of course, incorrect. Our e-services will continue to run smoothly, and more securely as well.

Cyber security is essential if Singapore is to become a smart nation. This is our aspiration. Cyber security is, in fact, a key enabler in our road to achieving our goal of becoming a smart nation. We believe that we cannot be a smart nation that is trusted and resilient if our systems are open and vulnerable. Stability in the cyber domain, regardless of whether it is a private, national, or international level, is achieved through stakeholder management. Stakeholders in the cyber domain include public agencies, such as government organizations; private parties, such as individuals and corporates; as well as international entities, such as the different countries.

The whole idea that the chain is only as strong as the weakest link is true, definitely in the cyber domain. The lack of coordination between these entities could also undermine stability. Systems like these could collapse when just one in a chain of highly interconnected stakeholders are hit. Chain reactions could cascade into system-wide paralysis within the cyber domain, and even have effects in the physical domain. The cyber attack on a Ukrainian power grid is an example of the fallout from the cyber physical domain.

Appropriate stakeholder management results in coordination, enabling them to act collectively with a system-wide perspective. This allows for mitigation of threats to the cyber domain comprehensively, on a system-wide level. For example, regulations for business to employ Managed Security Services (MSS) or for individuals who subscribe to upstream data inspection or world guarded measures at Telco level could potentially block initial malware infection. This could also disrupt

the cyber kill chain upstream, and possibly isolate cyber physical impact. All downstream stakeholders could benefit, and the overall system stability is enhanced. Such a system would be stable, shock resistant, and less prone to successful cyber attacks.

Stakeholder management does not mean a simple aggregation of individual plans. It means ownership, and a formation of a coordinated, private, national, and international cyber security system. That is bigger than the sum of its individual parts; it means system optimization, and not optimization at the individual or subsystem level. It should permeate every level, regardless of whether the interested parties are private, national, or international stakeholders. In fact, cyber security stakeholder management should be viewed as a holistic effort.

Within the national cyber domain, public sectors also need stakeholder management. Stakeholder management begins with the private sector stakeholders, specifically the formation of a domestic cyber security agency. Cyber security cuts across agency responsibilities and turf lines, and to successfully implement this, strong governance and the ability in public sector stakeholder management are required. This was the case when Singapore established its cyber security agency, CSA. Leading up to the foundation, I had the privilege of sitting in some of these high-level discussion meetings, and there was a heated debate about how CSA should be organized, and what its responsibilities would be. When I was listening to these debates, it was clear to me that no one in the room actually knew what the problem was, but everyone knew that the solution was to form CSA. I said good luck to whomever will have the chance to lead this new agency, and it came a bit of a surprise to me when they informed me later on that the ministers had decided that I would be appointed the chief executive of the CSA. This is over and above my other appointment in the ministry of defense that I hold currently.

The Singapore government was unified in vision and action to create the CSA, it houses both policy making and operational functions of cyber security in one organization. Individual agencies and ministries gave up all of their responsibilities, and even some of their expert personnel, to CSA. A firm foundation was laid on which to build up CSA's capabilities rapidly, rather than ending up in deadlock due to failure in public sector stakeholder management. Private sector stakeholder management is crucial for achieving stability in the cyber domain. Most

Critical Information Infrastructure (CII) is in private hands, some of these companies are not even local companies based in Singapore.

One way to achieve stakeholder management is through legislation; it coordinates the actions to create a stable, shock resistant cyber domain. Some examples include requiring CIIs to subscribe to MSS and other measures, such as accredited penetration testing. Private sector stakeholder management occurs across CIIs as well. In Singapore, just two months ago we mounted our first multi-sector cyber exercise, it was called "Exercise Cyber Star", it involved over one hundred participants, comprised of sector leads and critical information infrastructure owners from four sectors, namely the banking and finance sector, the government sector, the energy sector, and the infocom sector. Exercise scenarios included web defacements, widespread data exfiltration, malware infections, large scale DDoS attacks, as well as some cyber physical attacks.

Trying to get CIIs to share information and trust each other within the same sector is already challenging, and trying to do this across different sectors is even more so. It took substantial efforts in private sector stakeholder management and coordination to execute our exercise successfully.

Private sector stakeholder management must begin on a daily basis, not just during a crisis. We need to establish procedures to work together, share information safely and securely, and most importantly, we need to build up trust. All this must be done on a regular, day-to-day basis, when there is no crisis. That way, when a crisis does hit us, we already know what to do and we have a store of goodwill, trust, and confidence in each other, which will get us through the crisis together.

International stakeholder management is also crucial for extending stability into the international cyber domain, Memoranda of Understandings (MOUs) could achieve this. Singapore has already signed cyber security MOUs with France, the UK and India. Deeper international collaboration beyond MOUs is desirable. Singapore's Prime Minister, Lee Hsien Loong, visited Israel in person only two months ago. He highlighted our ties in technologies and R&D collaboration, and cyber security is one of the areas in which he wishes to deepen our relationship. Strengthening international collaboration is part

of international stakeholder management, it is necessary due to the borderless nature of the cyber domain connecting the world.

Cooperation and collaboration aid in mitigation of cyber threats, and enhance stability in the international cyber domain. International stakeholder management has to keep pace with advancements in technologies. Countries, corporations, individuals, and even devices are set to experience an unprecedented level of connectivity with the Internet of Things. CIIs are no exception, in fact many of them ride this wave: from supervisory control and data acquisitions, start-up systems, to autonomous and Cloud-based technologies, CIIs are being connected more closely than ever before, and it will become increasingly difficult for countries to secure and stabilize their cyber domains within the country. I will explain this in Singapore's context.

Singapore is an open and globalized economy, we have benefited tremendously from the rise of the internet, which fundamentally changed the way that we communicate and conduct business. We have a well-developed infocom infrastructure, which powers much of our physical and digital economy in Singapore. Many Singaporeans are digital natives. At 82%, we have one of the highest internet penetration rates in the world, and our mobile phone penetration rate is 150%, which means that most people, including myself, have more than one mobile phone. However, such pervasive interconnectivity also possesses significant threats to our computer systems and CIIs.

Across southeast Asia FireEye reported 29% of their customers were targeted with advanced cyber threats in the first half of 2015 alone. In this environment, where Singapore cyber domain is under constant threat, the Singapore government recently implemented a new policy to segregate internet surfing. Despite what you may have heard on some of these media reports, Singapore did not cut off the internet, nor did the government disconnect from the internet, it was a simple defensive move.

In the past, some of the Singapore government networks were very open, you could have full access to the internet, surfing and downloading from our work computer. Imagine what kind of threat this represents. The Singapore government plans to simply limit the ability to surf and access the internet from the office networks, a simple move to limit the attack surface to protect our systems and the citizens' data.

However, it attracts much inaccurate attention from the media, almost as if some of the media didn't want to understand what was going on, and preferred to tell a more interesting story.

When a cyber attack occurs in Singapore, the impact can not only be felt in Singapore, but potentially globally as well. Singapore's historical role was to be a transit hub for trade. Today we are a financial hub, a shipping hub, and an aviation hub as well. A successful attack on Singapore could affect global financial systems, civil aviation, and air traffic control systems, with disproportionate effects on similar critical infrastructure and real-world effects in other countries. This is because we are all now linked through what some people are calling super-national CIIs. These are networks that transcend borders and link together critical systems, such as the financial system, telecommunication systems, air traffic control systems, and so on. Against this backdrop, the need to cooperate for cyber security is even greater.

We need to recognize the urgency of the issue, and start working together to take action based on our common security Interests. As our cyber interdependence rises, so must our ability to protect our super-national CIIs. International stakeholder management is required to overcome challenges in collaboration for super-national CIIs, primarily because super-national CII's are, more often than not, also national CIIs.

There may be competing interests and issues of national concern between countries. As such, I would like to offer three proposals in managing stakeholder relations in the international cyber domain. How can we protect ourselves? First we must establish platforms for discussion, such as conferences, so that we can build trust, facilitate cooperation, and reduce the chance of miscommunications between countries.

Secondly, we should also aim for fair inclusive rules of the road, such as agreeing on the management of the internet as a global commons. We think that this will be best done by discussion at global institutions. Singapore also advocates a cyber space, where behavior is governed by the global values of social responsibility and consensus building, so that cyber security can be an enabler of smart technologies that improve lives and provide economic opportunities for all.

Finally, we must set some common goals to work towards, such as combatting cyber crime. In this are Singapore plays a facilitating role as a voluntary lead shepherd under the hospices of the Asian ministerial meeting on transnational crime. On the global front, Singapore also hosts the Interpol's global complex for innovation, which supports international cyber crime fighting operations. We hope that more countries can join us in fighting this growing threat.

In conclusion, we have seen that there are many forms of stakeholder management in the cyber domain, be it at the private, national, or international level, all are necessary as part of the continuous holistic effort in stakeholder management, and ensure system-wide coordination and the achievement of stability in the cyber domain in its totality, if we look at it from all three levels. Singapore recognizes that we can play a useful role in the cyber domain by fostering discussions on our common security interests on this new global commons. We hope that all countries can join us, and that together we can build an open and secure cyber domain.

JAMES ANDREW LEWIS, SENIOR FELLOW, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (CSIS), USA

Why do we need to think about international stability, and what does that mean? One way to think about this is that there is no technical solution to cyber security; that is something we should know by now, especially after Snowden's papers. You can do things to minimize risks and mitigate risks, and it is very important to do so, but there is no technical solution.

Somebody from Google told me once that Google has the same capabilities as the NSA, and I said that this was really cool, I had no idea Google had nuclear submarines. Governments have unique capabilities, and so thinking about how to minimize risk means that there is no technical solution, it has to be a political solution. However, it also has to be a transnational and international solution. There is no national solution, because this is a transnational threat. Most of the attacks will come from outside your borders, requiring a political international solution, which points to the UN.

One of the changes in the last few years has been a tremendous revolution in how people think about the internet. In the past, we had this

millennial vision that it was global commons that a multi-stakeholder model could control, and that governments would be less important and borders would be nonexistent. Unfortunately, that vision turned out to be largely wrong. Someone said that we had seen the end of history... well, history is back with a vengeance, and this means that we now have to think of this in terms of national approaches, where states are the most important actors.

Sometimes people say that we need the multi-stakeholder model to apply for international stability. There is a role for it, but at the end of the day we are talking about states, not companies or NGOs. Sometimes people say that we need technical experts in these negotiations, and I say: we need technical experts in these negotiations as much as we need vegetarians, meaning – we don't. This is real diplomacy. When we see technical experts in the room, they are very often baffled, and I know that some of them are upset as well. The internet used to be something that they dominated, and now states have become the most important actors in it, so no technical solution is required, but international politics. I think in that sense, almost inadvertently, the most important form has turned out to be this UN group of government experts that comes under the committee for disarmament and international security.

In 2010, after some rather intense discussions, the GGE, a group of government experts, managed to agree on eight lines that set the negotiating agenda that we have followed ever since. They said that the international community should develop norms for international peace, security, and stability in cyber space. They should develop confidence-building measures that include exchange of information, among other things, and that they should build capacity among nations around the world to improve their cyber security. This has set the stage for the last six years, and it still continues to be the negotiating agenda.

Capacity building has sort of spun off and become a cottage industry. Everyone loves capacity building, because if you are a big country, capacity building gives you a chance to tell other countries what to do, and if you are a small country, you hope that you will get some money, but the difficult part turned out to be norms. From the aspect of confidence building measures, there has been progress in the ASEAN Regional Forum in the Organization for Security Cooperation in Europe, and while we are seeing good progress in confidence building measures, norms turns out to be difficult, and the most difficult of

the norms turn out to be the application of international law. 2010 set the negotiating agenda, 2013 saw international agreement on the political principles that guide state behavior in cyber space, and those principles were the primacy of the UN charter, that all activities in Cyber space fall under the UN charter; the primacy of existing international law. This agreement embedded cyber security in the context of state relationships. And then there is also national sovereignty.

Between international law, the UN charter and national sovereignty, we have put cyber security in the framework of state-to-state relations. But what about non-state actors, private groups or hackers? These are important to think about, and it is a difficult issue because one of the problems with cyber security, which we hear about over and over again, is that it spreads over our traditional definitions: is it arms control? Is it non-proliferations? Is it state-to-state? The answer is sometimes yes, sometimes no. However, the primacy of states, both in being responsible for the security of their citizens and in possessing the most advanced modes of attack, puts the focus on state behavior.

In 2013, the principles were laid for what we would do in negotiating for international stability, and I think that there is a bit of a surprise here for people who track these negotiations, like me, because it turns out that the agreement that international law applied was exceptionally difficult to implement. And that would be because there is a fundamental dispute in how we think about cyber security, and that dispute revolves around these issues: is a cyber attack like a weapon of mass destruction (WMD)? And if it is a WMD, should we stigmatize and ban it? The model here might be the treaty on the peaceful use of outer space, which says no weapons in space, and some people have said – and it isn't an unreasonable position – if there are no weapons in space, there should be no weapons in cyber space.

The alternative approach is, of course, that cyber is like a conventional weapon, something that states will use and acquire. At present, many states are acquiring offensive cyber attack capabilities, and therefore we should embed it in the laws of conflict and in international humanitarian law, which will say that we can use this weapon, but that it has to be used with the concepts we find in the Geneva Conventions and the Hague Conventions.

These are two very different approaches, which constitute a fundamental problem in defining the kind of weapon that is cyber. There are those who want to ban and stigmatize it as a WMD, and those saying that it is just a conventional weapon that should be allowed to use, subject to proportionality distinction discrimination and all the laws that apply to warfare. That is a serious issue, because cyber weapons and cyber attacks can have strategic effect. It may not have a mass effect – in some ways, cyber attacks are more like a precision guided munition (PGM).

We have an old notion that cyber is like a worm or a virus that will spread globally, but that is not how it works, there are specific attack targets. It is a PGM, but it can still have strategic effect, if I target your electrical sector, your banking sector, your nuclear command and control, and so on. One of the underline tensions here is that we have created a new way of waging conflict that doesn't really fit into our WMD model, even though it can have similar effects to a WMD; it doesn't really fit into our conventional weapons model, because it can do more than a conventional weapon; and so, the international community is wrestling with how to deal with this, and there will be another GGE this year, starting in august, which will look at these things. I think that they will reach an agreement, but I don't know what this agreement include.

This is a fundamental dispute, and some of the issues that come up are, for example, what is an attack? There is a strong desire in the international community not to define "attack", and that is a dilemma, because so much of international law is predicated on the notion that anything above the determined threshold is the use of force, and anything below it isn't the use of force. This is how you decide that something is considered an attack, or that the use of force is crucial for applying international law in the UN charter, but nations don't want to agree on this. There is an implicit understanding that any cyber action that results in physical destruction or human casualties will qualify as an attack, but there is clearly a gray area, like in the case of the Sony attack.

What was Aramco, when data was wiped and hard drives were destroyed, was it an attack? Stuxnet was clearly an attack, but Saudi Aramco and Sony fall into a gray area. One of the problems here is coming up with a solution to apply international law to develop how states

behave responsibly, when we can't even agree on what is an attack or a weapon, or any of the things that would apply to conventional warfare.

Another thing we are wrestling with is that while the GGE was a very valuable vehicle in the last six years for making progress, it may have reached the end of its utility. I think that there will be agreement in the next year, but we need to think about what will take its place, and there were suggestions to move this issue to the committee on disarmament; to create an open-ended committee, like the committee on the peaceful uses for outer space; but there is no agreement on this. What we have is a situation of definitional problems, and disagreement over what the venue in which we discuss them.

It is probably the time to move to some kind of formal agreement – this will take years to develop, but we need to start thinking about what a formal agreement among states on international security would look like. It is probably the time to think about how we can embed this in the UN framework. The GGE is a proxy approach, but we need the UN, we need a formal agreement. One way to think about this is that we have formal agreements and institutions to manage stability for the monetary system – the IMF the IFFYS international financial institutions. We will probably need to move to something like this for cyber security as well. There is no technical solution, we need to find a political solution, but we are at a very early stage of coming up with this agreement.

KIM WON-SOO, UNDER SECRETARY-GENERAL AND HIGH REPRESENTATIVE FOR DISARMAMENT AFFAIRS, UN

There are three points I wish to discuss. First, I would like to talk about the GGE, what it has been doing and what it is going to do. GGE has been very unique on cyber security. The UN is a global platform to discuss and devise a normative framework for the international community, and it has 193 member states, but because of the division on the fundamental vision of what should govern cyber space, our member states couldn't even start deliberations, and instead they asked the Secretary General to compose a very small group of government experts.

Ten years ago, we started out as fifteen people, and the next GGE, the fifth of its kind, will include 25 members, and I thought that the

number should have been expanded to at least 30, to accommodate a slightly larger number of member states. However, it was not possible, because it is still difficult to build on the list of common denominators. In the last GGE, in 2015, we identified a number of issues; however, even though we agreed that international law must apply to protect critical infrastructure, we still we do not know what kind of critical infrastructure should be protected, not only in times of peace but also in conflict situations. We also don't know what kind of law would be applied, which will include both international humanitarian law and international human rights law, because there are still two contending imperatives – privacy and freedom of expression on the one hand, and state security on the other hand. Which of the two should take premise?

These underline tensions still constraint the ability of the GGE to enhance the common denominator of a normative framework, although we all agree it should be voluntary, and not legally binding; it should be politically binding, but it is not easy task for the future. Personally, I feel very sorry that the GEE is unable to accommodate more than 25 people, including several member states who have very strong IT capabilities and expertise, which they can offer for the future work of the GGE, but that is the reality we have to live with.

My second point is the urgency, as accentuated by what is known as the warfare ABC – atomic, biologic, chemical. At the UN we use the abbreviation CBARN – chemical, biological, atomic, radiological, nuclear. Through several exercises involving the highest level of governmental leaders through many forums, such as the nuclear security summit, whatever scenario-based exercise we do always involved three elements: CBARN material, theft by terrorists, and using cyber. This is our way to fill the normative gap we have. It means that terrorists or violent extremist will thrive, because they always stand ahead of the curve, and because of the division of member states on those critical issues, international committees tend to stand behind the curve.

My last point is the need to ensure coherence in various multilateral forums and initiatives, and deflect that fundamental difficulty in the contending imperatives. No matter on what forum – internet governance, digital economy, global information, world society of information – it is not easy to come up with consensus views, but because of the important breakthrough made by the last two GGEs, that outcome is now being cross-referenced by other forums. Therefore, whatever

we are doing at Track 1 or 1.5 or 2 of diplomacy, we need to ensure that all our efforts can help each other in a mutually complementary and reinforcing way, rather than mutually competing. Otherwise, those states who have different views will continue to shop between the forums; we call it forum shopping. This will delay the consensus building by the international community.

We hope that whatever efforts we are making with the private sector and the government, the business industry and the academia, we hope all those insights will be channeled through the GGE, so that we will be able to enhance the level of the government framework we are going to have for the future. We know that all of these tasks are very challenging, and require very intensive and creative thinking out of the box by all stakeholders and at all levels, meaning the global level, which is the UN, but also regional and sub-regional levels, where organizations like OSEE and the EU, as well as many other regional, sub-regional, and national organizations. This should also apply to governments, the private sector, industry, business, and academia.

I hope that the initiative taken by Israel by organizing this type of conference will be emulated by other countries in other regions in the months to come, before the next GGE starts its' work, and also in-between the sessions of the GGE, which will meet every 6 months for a week, and many things can happen between sessions. We also see an increase in the willingness of many countries to organize similar events, and an increase in the number of key states that help us in devising the way forward together. I think that our joint efforts will lead us to building a world that is safer, more secure, and also more open and accessible for everybody to use peaceful IT, infrastructure, and technology, and we count on all of you.

WILLIAM H. SAITO, SPECIAL ADVISOR – CABINET OFFICE, GOVERNMENT OF JAPAN

When speaking of stability in the international cyber domain, I would like to address the concept of redefining this trust. The internet has existed in some manifestation form since 1969, it isn't a recent thing or a phenomenon, and if we look at the history of the internet, we can see a huge growth or uptake in the internet. However, my argument here is that although it was a catalectic, it wasn't necessarily the invention

of the World Wide Web that created the adoption of the internet. My hypothesis here is that around 1995 there was a catalectic, the advent of the Secure Socket Layer (SSL), compounded with RSA becoming publicly available in 2000, this is where the internet was starting to be adopted rapidly. I bring this up because it isn't ICT that is driving security, but security that is driving ICT, security is the fundamental enabler of the internet, which allows everyone here to do what they do.

Before this widespread adoption, the internet was an academic tool, a means of open communication, it was never designed for this. It was cyber security that evolved and innovated, and allowed the internet to become a business tool. The counterpoint of this is, of course, that if security does not keep up, the internet and its growth and its utility to society will stop. This is a concern, especially with one of the reports that just came out in March 2016 – this report is one of many, but it highlights this issue. It was released by the Department of Commerce, and it was a three-year study. The highlights of this report show that in the USA, for example, 45% of internet users are curtailing or changing their online activity due to lack of confidence and security. This is frightening, because here we spend all this effort and energy to create this great infrastructure, this great tool for mankind, yet already significant portions of the populations are becoming afraid of the internet, and changing their activities.

As a country and as a global audience ,I think it is very important to understand that we are at the cusp of seeing this get away from us ,but we have an opportunity to fix this .Having said that ,in my25 years of worldwide activity in the various fields and sectors of cyber security ,practical ,managerial ,educational ,and political ,I have noticed something in talking to professionals in this industry for quite a long time ,and we call this the ABC of security :A for atomic ,B for biologic ,and C for chemical .Looking at the GGE ,many countries try to and tend to relate to cyber security within the framework or the metaphor of this ABC ,but if you look at it and talk to many people, asking why we are really struggling with this concept ,you'll see that the next letter ,D ,for digital ,is causing lots of headaches and turmoil. The reason for that is simply because D is fundamentally different ,and it is sometimes dangerous to apply the ABC principles to a D concept.

Without going into too many details ,it is obvious that cyber is not constrained by physics ,it moves at the speed of light ,quite literally.

It can happen anywhere ,but also what is interesting – which is not possible with all the other ABC – is that it can happen simultaneously. From what I see and hear talking to people and listening to their concerns ,we no longer have a cold war ,but a code war .I think that while GGEs and Track 1 discussions are very important ,our issue here is that while in ABC we had somewhat rational actors that are able to talk and discuss those issues in decent ,formative ways ,in D ,non-state actors and other professionals also play a role ,which has changed the rules and made things different and more difficult than in the past.

Personally ,I think that when we are discussing cyber security ,we are currently in a" Track "1.5 type of world .Attribution is obviously an issue ,and at the same time the attacks are very asymmetric :we can spend a lot of effort defending our networks ,and even if we are able to attribute the attack to specific attackers ,the traditional means of retribution may not be as effective because of the asymmetric nature .The asymmetric nature in the cyber domain has many different aspects ,another one of them is how policies progress here – in ways that are sometimes frightening and sometimes interesting .Just last week NATO had just announced and recognized that cyber is another domain ,and it is now treating cyber as a warfare dimension ,just like air ,sea ,and land.

We live in very interesting times ,where we can see the progress here, see the cyber evolving both at a policy level and a technical level ,not necessarily in sync .This year Japan was the host to the G7 presidency. Unfortunately ,until now ,in dialogues like the G7 and G7 summits cyber security did not take that great a role ;last year I think we had about a paragraph .I am proud to say that in this year's G7 ,cyber security was reflected with 505 words ,which is about a page and a half ;but it is important to note some of the key terminologies that we are using there .It is understood that there are non-state actors that have to be dealt with ,including terrorism ,but it is also important to understand how this fits into the context of international law ,and this will be an ongoing issue not only for the G7 ,but for other countries as well.

I can't emphasize this enough: having been in this industry or over a quarter century, I can see that the actors are definitely changing. When I started out in this industry maybe it might have been a little bit too early. The players were script kiddies, teenage hackers, people

who wanted notoriety, as well as the people that just wanted to cause headaches. Many people still think that cyber security is this realm, but it has completely changed. Now there are well-funded professionals, who are persistent and are in there for different motivations. To make matters worse, the outcomes and the developments that these people do, the millions of dollars that they people spend on R&D, can quickly be recycled and used basically for free by the other actors in this system. Therefore, I argue that while Track 1 diplomacy and Nation States and discussions are very important, a major part of the damage being caused these days, which threatens the general public, tends to be Non-State actors, and we also have a dual mission here of addressing this issue.

The other issue that I am concerned about is that many policy makers, governments and people in general tend to think of cyber security as a logical attack ,while this is not the case .It is clearly a kinetic ,physical issue .Cyber does not necessarily mean logical ,and given that Japan will be hosting the Olympics in ,2020 this is a concern of mine ,where cyber is clearly linked to other risk issues ,including physical ones. I think not only from a nation state perspective ,but companies and individuals as well ,these things will just be a growing concern that we need to address.

On March 2011 Japan suffered the second largest recorded earthquake in human kind ,and we had a nuclear accident .I was asked to participate in the national investigation of this accident ,and although I am not a nuclear expert ,being of a cyber background ,I tried to understand the genesis of accidents ,risks ,and these kinds of threats .What I found was that when you look at historical accidents and incidents, both nuclear and other big recorded events ,you notice three common attributes :one ,people make mistakes ;two ,machines break ;three, accidents happen .This is important to know ,because people need to realize that in our complex world ,there is no such thing as 100% proof or safe ,that failure is normal ,and that things break .For this reason, I am also now harping on the importance of this concept of resilience.

Resilience can sometimes be a very cultural issue ,because some people have great difficulties to comprehend this concept ,especially when you go for perfection .In 1998 I was asked by the federal reserve to be part of a commission for the year 2000 problem) Y2K ,(and we tried to solve the problem .As many others ,we have spent millions

if not hundreds of millions of dollars overcoming this problem ,and the world continued to exist .However ,immediately right after the Y2K problem was done with ,we were questioned by many people in authority who wondered ,was that really necessary ?Did we need to spend that much money ?Did the Y2K problem even really exists ?This reminds me of cyber security today :if you don't do it you are screwed, and if you do it you are screwed anyway.

What was interesting about this ,though ,was that a short time after the year 9/11 ,2000 happened ,an attack on the financial institutions of the USA ,yet the Dow Jones came back ,and people were able to get cash from their ATM machines relatively quickly after the event. The amazing thing about this ,which I was able to see firsthand ,was that minutes after the 9/11 attack ,the financial community pulled out the Y2K manual and ,based on it to create the resiliency to get back the financial systems of the USA .This is extremely important ,and the point and the moral of this story is that cyber security can be the resilience for a country ,that helps it to not only become stronger ,but can also be useful in other areas.

Another concern ,and using Japan as a metaphor here ,is that competitiveness and efficiency are very directly related to ICT .If your country does not get ICT ,it will be in dire straits .Yet many people, companies and organizations and countries ,do not implement ICT, because of their fear of cyber security .It is important to get past this ,and to understand competitive issues .This is not just a negative whack-a-mole ,competitiveness is extremely important for us in order to go forward.

Additionally ,if done correctly and by design ,security makes many other things better ,it increases performance and efficiency ,and it will become a differentiator for not only countries but businesses, products and services .In order to do this ,security has to be thought of as a triangle ,which many people forget :security ,cost ,and usability. Obviously ,you want security ,and you want to do it in some kind of cost measurement ,but what many people forget when doing security –including countries ,but also companies and individual – is that you cannot give up usability .Many cyber incidents that I see around the world are not actually security issues but usability issues ,and so without understanding and balancing this triangle ,it is very difficult to do cyber security right .As countries ,this is very important to

understand it ,otherwise your companies and people can just copy and paste the server away and go elsewhere.

2ND SESSION: PREPARING FOR THE NEXT THREAT – CAN WE BUILD ECOSYSTEM RESILIENCE?

KEREN ELAZARI, ANALYST, AUTHOR & RESEARCHER, BLAVATNIK INTERDISCIPLINARY CYBER RESEARCH CENTER, TEL AVIV UNIVERSITY & K3R3N3.COM

Ecosystem resilience is a very important topic that we have been hearing about a lot, but what does it actually mean? I want to give you my ideas about ecosystem resilience and why we need it. The question that many ask today is, will the future be secure, and can we make it more secure? It is my personal opinion that by working together, we can secure that future ecosystem, and that's the vision that I want to present to you.

I am a senior researcher at the Balvatnic ICRC center, and it is through my work that I keep questioning what does the future of cyber security look like. Ten years ago, a depiction of the World Wide Web already looked like an ecosystem, almost like a living organism; however, if I wanted to depict what today's connected internet-cyber-physical world, it would look like a much more complex image, perhaps something like our very own galaxy, the Milky Way. Our digital world today is filled with black holes, meteors, and strange planets that we have never visited, and as we think about the expansion of this digital world – just like our universe that is continuously growing, not just on the linear scale but exponentially – it would be naïve not to think of the security considerations of that exponential expanse. Take for example a tool that I like to use in my security research, Shodan.io. This is a search engine that can identify connected internet devices, not just computers or smartphones, but also power stations, wind turbines, internet-enabled toasters, web cameras, and so on. It is a tool created by a hacker called Akilian, or John Matherly, and I think it is a fantastic addition to the tool kit of a friendly hacker, that you have

this sort of mapping technology to help us understand this expanding galaxy that we live in. Don't we need all the help we can get to make sense of this new world of our ecosystem? I think we do.

Consider software, new lines of code are being created every day by the hundreds of thousands, some of the most popular apps and operating systems have hundreds of thousands of lines of code. But what about the new operating systems? What about a modern car? Consider that a modern vehicle in 2016 has millions of lines of code, software that is built into a cutting-edge product that matters for personal safety and life and death. Would it be naïve to expect a car company to make sense of all that code, especially if you consider that they don't actually make all of that code themselves? We already live in a connected ecosystem; companies that make new products, whether they are mobile applications, cars or coffee machines, use software assembled from paths made by different companies, third parties, different nations; this is the issue of software supply chain that we often hear about. So, with this supply chain, don't we need more people to help us find the issues?

I have always been inspired by friendly hackers. In fact, the woman that first led me to fall in love with the hackers' world is someone you might recognize – Angelina Jolie. Twenty years ago, she portrayed a young fierce hacker called Acid Burn, in the movie *Hackers*. I was fourteen years old at the time, but when I saw that movie I fell in love with the idea of friendly hackers that can be the heroes. Today, that idea of hackers as heroes is becoming closer to a reality more than ever before.

Two years ago, I presented my idea about hackers as the immune system for the information age on the international Ted platform. I am glad to say that the idea has become viral into itself, meaning that I wake up in the morning and I get messages from hackers all over the world – Africa, South East Asia, North America, Europe, Japan – and these hackers write to me and say that they want to be a part of the solution, not just a part of the problem.

How can hackers act as that immune system? How can they make us all build a more defended future for everybody? In the past year I have taken upon myself a research project to look at how hackers are helping us defend against the real bad guys, and guess what?

Those bad guys are not criminals or Nation-State spies, they might not even have a face. However, they have a name. That name can be Heartbleed, for example, like the open SSL fundamental flaw that was discovered a few years ago; it might be a bug in USB technology; it might be a bug in Unix operating system, like the Bash Shellshock vulnerability. The common thing in all of these fundamental software vulnerabilities is that they are not discovered by the people that make the software; in fact, they were reported by independent security researchers and hackers working for different teams around the world to identify problems and code.

In 2016, I like to say that life is just like a box of chocolates – you never know what you are going to get, especially when you assemble your code as a puzzle made up of different pieces. Would it be naïve to inherently trust that code without testing it? Shouldn't we have all the help we can get by engaging with hackers that can help? As long as humans write code we will have bugs. In fact, even when AI and robots write codes, software vulnerabilities will pursue. We can debate on many software vulnerabilities we will have in our future but the reality is that these are the real bad guys that we need to defend against, not independent hackers. That is why in my research work I have been focusing on those hackers that engage in bug bounty programs.

Bug bounty programs are not new. They have been around for more than twenty years, but in the past few years they have evolved to include some of the biggest companies in the world that you may have heard of, like Uber, Western Union, Tesla – all of these organizations have learned to harness the power of friendly hackers to identify software vulnerabilities. Personally, I think it is a great way to make our ecosystem safer, but that is not the only story there. There are also personal stories.

Perhaps you have heard of Nir Goldshlager, one of the hackers that manage to hack Facebook all the time. In fact, Facebook has announced him, year after year, as one of the top 5 and top 3 hackers. But Facebook does not pursue criminal charges against Nir, in fact they reward him for his efforts, because he is one of the Israeli security researchers that have helped Facebook and anybody that uses Facebook be safer by contributing to their bug bounty program, one of the biggest bug bounty programs in the world.

Facebook is not the only company doing this; most technology giants are harnessing that power of friendly hackers, which is why 2016 is a good year to take a look at what has happened in bug bounty programs, and ask how can we derive more value from such programs in the future. Innovative companies, such as Tesla, bring their flagship cars out to DEF CON, the world's largest convention of hackers, so that they can engage with the security research community. We are also doing it this year in Tel Aviv with the B-sides security hacker community event .Even the pentagon has recently announced a bug bounty program ,actively inviting hackers to show them how they can be better and safer.

Hackers are not just the bad guys out there ,and in fact these programs represent a great value for the companies that run them ,and in the past year I have been asking myself what is that value is one ,and looking at it with my research .Here are just a few early insights from what I have discovered :security researchers that engage in bug bounties help companies find more bugs faster ;security researchers and companies that engage in bug bounties raise awareness and media attention ,and create better reputation for themselves and for the companies when they engage in bug bounty programs .And here is the most unexpected phenomenon of them all :bug bounty programs are creating a potentially huge impact on the future workforce of cyber security ,because people from new parts of the world ,that have never before been legitimately rewarded for security research work ,are now engaging in a new global ecosystem protection effort and bug bounty programs .For example ,if you use Google's products ,friendly hackers are already making you safer .There are friendly hackers not just in Europe or North America or Israel ,but also in Africa ,the Middle East, the Far East and South East Asia.

That is my wake up call for thinking about ecosystem and ecosystem resilience .Hackers are not always the enemies ,and it takes adaptability to think differently ,to go beyond our limitations ,and engage with those people that we usually are afraid of.

DR. YANIV HAREL, GENERAL MANAGER, CYBER SOLUTIONS GROUP OF EMC; HEAD OF RESEARCH STRATEGY, BLAVATNIK ICRC, TEL AVIV UNIVERSITY

First of all, I would like to talk about the Target breach, which was one of the most important events in the last few years – not the most sophisticated event, or the event that used the most complicated tools, but the one that changed the world, and made commercial companies understand that they might also be targets or destinations for this kind of breach or attack. In the Target event, about 50 million credit card numbers and other credentials were stolen and went from the secure perimeter of the company into the open market. I would like to review the technical environment of this event.

If we try to analyze this event, we can understand that in the Target event it wasn't targeted specifically; it wasn't initially attacked. One of the sub-contractors of Target, not even Target itself, was initially attacked, and later on after the attackers succeeded in reaching the Target network by "jumping" into it. However, if we try to focus on the Target network, we can analyze the process of how the attackers jumped from one point to another, started to reach and to gain control or take over assets inside the network. Later on, they skipped to the other server while taking the information with them, from there they continued to another sever, and then to a drop site that was located outside of Target's network, and all the way to the attacker, the one who managed this process.

When we try to analyze this event, we should ask ourselves if it is possible to prevent such event in the future, and this is part of our challenge. In the past, our industry was built on antiviruses and based on the idea that we are familiar with the signatures of the viruses and the attack tools of the attackers, and then we can send the signatures to all the end-points that have the antivirus to stop this attack tools from penetrating. However, today we can say that we are fighting the unknown, attack tools that we are not familiar with, so we have to think of other ideas. Today we invest our efforts in anomaly detection, in trying to prevent, in trying to shorten or limit the damage, and so on.

I would like to discuss here the idea of simulation, because we believe that operational simulation is also something that can be a part of our campaign to prevent those attacks, and we invest a lot in this

capability. Imagine that we can take a blueprint of our network or a segment of it, and run simulations of attacks prior to the attacks themselves, in order to understand what can be the circumstances for the attack, and if we are vulnerable against them. If we have such a capability, I claim that we can prevent attacks like Target and others: if we try to find and to run all of the attack paths and ideas, or at least the relevant ones that could attack our system, we can then analyze the process, and find that if we change the authentication in our system, if we change the IDS or the IPS in our system, or if we change the DMZ, we can prevent such an attack. We can, of course, do the same for other attacks and potential attacks, and then to see the value before we face it in real life.

This is the simulation, and we at the cyber solutions group of EMC believe it to be an important and relevant as a service or as a turnkey project for our next generation of proactive defense capabilities. Our group is located in Israel, and at the federation level of the EMC group, we collaborate with all of EMC's companies, use their products as building blocks, and create solutions for the global market. Our home base is in Be'er Sheva, in the new ecosystem of cyber, academia, companies, and government organizations, and as part of that community there are many cyber capabilities that are being developed. Our group believes in collaboration with other companies, and we collaborate with large companies as well as with many start-ups. We believe that part of the innovation comes from collaborating with start-ups, and we combine start-up technologies in almost every solution we develop. We also believe that a part of the way to develop cyber is by working with the academia, and we have very good relations with Ben Gurion university, as well as Tel Aviv university.

However, it requires more than a simulation to solve the challenge of a specific organization or company. We also have to think about the problem of collaboration. Today we defend every organization and company only by ourselves, against all the threats that we can imagine; we have to find the way to collaborate as a community, and if a threat attacks one company, we can share this and defend other companies as well, as a community or as a sector, and enjoy the collaboration in order to be more protected. After all, the attackers are collaborating, so we, as defenders, have to find a way to collaborate as well, this is our challenge.

We believe that ideas for collaboration make us think about the idea of CERT, which is something that we started to develop about two years ago. The concept of CERT as one of the collaboration-related solutions that companies think about, and in this CERT, when you think about the challenges you can consider budgets, technologies, and other challenges. We found that the most important challenge is the conflict or the debate whether to share or not to share. This is really a challenge, although we all understand that collaboration is very important. To decide that I, as a company, share important information with others or with the public, is a really tough decision to make. We have to decide it, and to understand the risk. It is not an easy question, and we believe that this is one of the most important concepts, and that the CERT should provide value to the participants, so that they are willing to actively participate and share information and other ideas.

With this idea we started, years ago, to develop our CERT concept. We took our SOC capabilities, and we created the whole concept of SOC management platform. We also regarded our concept for CERT solutions, and defined the responsibilities that we believe a CERT should provide. In addition, we planned and designed the right set of components that we believed should be in the next generation of CERT, and defined the processes that we should have in such a CERT.

We were happy and to hear that the Israeli government issued the tender for the Israeli national CERT and we were proud to be one of the companies in the coalition that won this tender. At the moment, we are at the middle of this project, providing and implementing the Israeli national CERT as one of the vendors that implement this project for the Israeli government, as well as being chosen to be a part of the coalition for the sectorial CERT of the infrastructure, water and energy sector. We are in the middle of these two very important and very challenging projects, and we feel honored for being granted the responsibility to meet the government's challenges and expectations. As part of these challenges, we believe that combining the CERT capability and the simulation capability can yield a kind of new capability to defend against both known and unknown attack. We believe that we can go and start the next decade more protected and more ready for the next challenges.

To summarize, we believe that the cyber challenge is taking a very dynamic path, and will continue to challenge us for the next few years. We at EMC believe that we have to think about innovative ideas to face the unknown attacks and the very dynamic evolvement of the attacker side. In our opinion, the simulation is one of the ideas to do it, and collaboration will multiply the effect of our organizational capabilities to sectorial and national capabilities.

BEAU WOODS, DEPUTY DIRECTOR, CYBER STATECRAFT INITIATIVE, THE ATLANTIC COUNCIL, WASHINGTON DC

I took the idea of building resilient ecosystems and I wanted to play on it a little bit, because ecosystems – at least technical ones – are only a part of what we are trying to do. They serve a bigger, broader purpose, which is to build more resilient societies. Over the past 10-20 years we have been doing that through cyber-connected technologies, as kind of an underpinning. Over the last 50 years, in the USA alone, automotive safety engineering has saved over 610,000 lives on USA roads. We still have about 34,000 lives lost every year on USA roads, and about 94% of those are caused by human error – a mistake, poor judgment, distracted driving turning into the wrong lane at the wrong time. The promise of vehicle to vehicle or vehicle to infrastructure communication in autonomous cars, all underpinned by cyber technologies, can reduce those numbers greatly to a triple or a quadruple digit number of deaths. That would be an amazing thing, coming from 34,000 per year.

Similarly, in hospitals in the USA we have about 98,000 deaths caused by hospital errors – patients that come in for one reason and end up not going home for a different reason. In the late 1990s and early 2000s we decided to take that problem on, and we invented the concept of electronic healthcare records to be able to better keep tabs on what doctors are prescribing and how patients are being treated, and to get a much higher level of quality into the health care delivery system. More and more, the treatment is being carried out by connected medical devices, which promise to have the same types of exponential benefits as connected technology in other places – namely the ability to scale and automate with fewer mistakes and errors. A great promise can become a great peril, the same capabilities that can save and preserve life can also harm and end it.

I have a hacker friend who is diabetic, and he had an insulin pump until he found out that it was vulnerable to several different types of attack, and since then he no longer trusts that technology, and injects himself with insulin 10-20 times every single day. He has denied himself the best medical treatment available commercially, because he doesn't trust the underlying technology. Similarly, in talking with people in the congressional staffers talking about car hacking, they said that they don't care so much about loss of life, because 34,000 people die on roads every year. What was more concerning to them is that any crisis of confidence in the buying public would affect a double-digit portion of the American GDP, which is quite a large number.

As companies, who are investing billions and billions of dollars in smart homes technology and other internet areas, what does it mean if consumers are unwilling to buy those technologies for lack of trust? Earlier this year, the Atlantic Council released a paper indicating that about 66% of potential customers for internet-connected smart home devices had very serious concerns about the security of those devices. People with very serious concerns don't buy the devices they are concerned about, so what does it mean, if an expected $1.7T in global benefit by 2020 is erased because of the lack of trust?

There is also a lack of public trust in governments. Governments are supposed to keep us safe from bad actors, they are supposed to protect us from things that harm us in a systemic way. If they fail in fulfilling that promise, then people will drop out of the social contract. You will see more and broader social protest movements like Occupy or Anonymous, and it could even lead to Non-State actor groups and maybe a broader activism and more violent reactions.

A few years ago, some friends of mine started an organization called I Am The Cavalry. The premise was that our dependence on connected technology was growing faster than our ability to protect them, and when it comes to things like medical devices, airplanes, trains, and the failure rates we have in corporate IT are no longer good enough. The theory was that if we reach someone high enough in the government ranks, surely someone would have a clue, and there would have been working on solutions a long time ago. When we got there, we realized that this actually wasn't the case, and that we were the adults in the room. That simultaneously scared us and empowered us. Then we said, if the cavalry isn't coming to save us at the last minute, like John

Wayne in the movies, then that responsibility falls on us. I Am The Cavalry is a personal declaration that I will be part of the solution.

The second force that we have driving some of this failure modes or potential failure modes is vulnerability. All systems fail, engineers know that; all software has flaws, because people make mistakes. Software is coded by people for now, and we are liable to make mistakes. The question is how do we track vulnerability, measure it, resist it, and overcome it. In software engineering, we have a concept of defect density: there is a certain number of defects per thousand lines of code, and this is the scale by which it is measured, and people disagree over what that number actually is, but on a scale of a hundred million lines of code, like you have in mini modern automobiles, that still represent tens of thousands of systemic vulnerabilities that exists.

We also have another force that is emerging in vulnerability, which is the tendency to assemble systems from code components rather than to write everything from scratch, which is a good thing. It leads to more resilient code, because you find the flaws in it earlier. However, it also means that we are inheriting vulnerabilities from these lower-level code components into the higher-level systems, meaning that you can have issues where these parts are assembled. The final goods' assembler, the auto maker, maybe doesn't know all the vulnerabilities, or even all of the software packages that might be in their final system.

One of the third components of this is the increasing amount of connectivity. Software and isolation can only do so much. When you connect other software, it can do much more, it is much more powerful, however that comes at a cost of exposure to accidents and adversaries. In talking with some of the people from the automotive industry. they have compared this to whether or not your car is engineered to drive in an underwater environment, and of course almost no cars today are made to do that. However, cars' software was also not engineered to survive in an internet environment, and yet we are rapidly connecting those with 4G and LTE, and adopting apps. Just the other day I saw that many Lexus cars had their entertainment system shut down because there was some bad data coming from one of their third-party app suppliers, which caused the crash of the infotainment system, and incidentally also took out the air-conditioning, which can be uncomfortable, to say the least.

These are the types of things that can happen when you have this increasing dependency in connectivity, which we know that we have. We have increasing vulnerability measured in total lines of software code at a certain defect density, and we have an increasing exposure. Typically, at this point somebody jumps up and says, "all right, but we have this security model that we already know how to work, we can do this right?" and yet we know that nearly 100% of the Fortune 100 companies have lost Intellectual Property over the past few years. This is something that Richard Clark said in 2012 and it is still true today. We also have approximately 4% acceptable fraud rate and financial transactions, that is just the cost of doing business. As we depend more and more on these infrastructures that we have in the corporate environments, it is worth asking the question whether these are the acceptable failure rates in death toll, in public safety problems, or in public health issues; if patients are afraid to go to the hospitals because they think they might be hacked in the hospital. Personally, I don't think that we have had those societal level discussions. In the face of these uncomfortable truths, we need to look for unconventional approaches to solve them.

A couple of years ago I am The Cavalry published a 5-star automotive cyber safety framework. Earlier this year we followed that up with a Hippocratic oath for connected medical devices. The idea was not to have a prescriptive regime for technology controls, but to look at what capabilities, both technical and non-technical, are available that we know can help. We thought, if you start from the premise that all systems fail, what are your postures towards failure?

There are five common things that we found in parallel evolution of these, two lists that seemed to fit in these two places, and probably others in the Internet of Things, at least. First, if all systems fail, how do you anticipate and avoid failure? Second, how do you take help avoiding failure? Third, how do you learn from failure once you know it has happened? Fourth, how do you inoculate against future failures in that deploy fleet? Fifth, how do you isolate and contain failures?

That is the simple way to summarize what we found. Essentially, it breaks out to security or cyber safety by design, which is how do you look at the product development's life cycle and infuse it with a good degree of lessons from the practices that we know worked very well, such as adversarial resilience testing, or something like a formal

software security development life cycle. Secondly, taking help from willing allies or third party researchers. When GM launched its bug bounty program, within 72 hours they had triple digit submissions of bugs. Double digit of those were unique and severe. Within that same 72-hour framework they managed to fix three of them, that's how quickly organizations can move when they know about these flaws. If you think about it, 100 submissions in 72 hours, these couldn't have all come from people that bought new cars after the bug bounty program was announced, and then started to hack them. These were bugs that were already known, but that the researchers were afraid to tell the organizations for fear of law suit. When GM said: "we are not going to sue you", those researchers opened up and helped protect the public in a way that also protected themselves.

The fourth one, inoculating against failure, has to do with software updates. If you look at many of the update processes that happen in Internet of Things, as well as some of the other technologies, you actually have to go and replace hardware. Think about the difference between a software update: whether it is over the air like we have on our phones or through a manual process, a software update requires that you learn about a flaw, you fix it through software, and you develop an update for it. To do a hardware update you actually have to manufacture new systems, go in and do a physical replacement, which means it takes orders of magnitude more time to be able to do these things. And looking at the medical device industry, if you think about what it might take on a timeline of a medical device to replace these systems if you don't have the ability to patch them, it can be years, not weeks – that is a long time to be out there exposed.

Finally, we have compartmentalization and isolation, segmentation. If you think about a submarine, when one of its areas is punctured the sub doesn't sink, because they have ways to segment that off. The same happens in software. When your infotainment system goes down because of bad data or because of a malicious attack, it should not also have the capability to take out your breaks. Severing those links that exist today might be a good way to protect against this. A second, unconventional approach, is something that was proposed in 2014 by congressman Royce, which was the Cyber Supply Chain Management and Transparency Act. Essentially, it said that we need to know all the third party code components – things like a bill of

materials for software or a food label nutritional information, to know what the ingredient list is. There should be no known flaws in the software, or if you do have flaws, it should be for a very good reason. It should also be software updatable – once we know about the flaws we can fix them.

This act didn't pass, but organizations like Mayo clinic and the underwriters laboratory have begun to adopt these things voluntarily. Another idea is to be able to bring some type of a regime to hold final goods manufacturers, in good faith, accountable for some of these things. There is a famous case of McPhersons versus Buick motor company: back in 1916, where Buick was assembling the car, a guy named McPherson had a defective wheel, and the courts found the Buick motor company was liable for his injury, because they were in the best position to be able to eliminate defects throughout the supply chain. If we are not already looking at these things now, we must start soon, otherwise bad things can happen. Take the fire on the Cuyahoga river in Ohio in the 1960's as an example. The river caught fire because of all of the pollution, and it stayed on fire. It hit the news cycle and it triggered an inevitable reaction from policy makers, who overnight put in place a sweeping environmental regime. That is very good thing in a long term, but in a short term it had some severe limitations; it hurt businesses, and it actually was a little counter-productive.

If we don't have good clueful response mechanisms in the face of a disaster like this, ready to go, we won't be able to survive, we will have more harm done than good, and some people have told me some of the things that might happen would be extinction-level events for the software industry. We need to start thinking, planning and acting now before it's too late.

ORI EISEN, FOUNDER & CEO, TRUSONA

Today I will take a little trip down memory lane and show you that the crimes we fight are not new at all. Identity theft started back in the bible. I chose to talk about this topic in order to change something in you. When I asked myself "where does the money go?" my life changed. When I was head of risk at American Express, one day I asked my boss: when we lose $10M, where does it go? Recently we heard about $81M that were stolen through the Bangladeshi bank

over SWIFT, where did that money go? The answer is, this money goes to five things: narcotics, weapons, terrorism, human trafficking, and the worst of all – child exploitation.

The internet today is all about convenience. Nobody wants to take the extra step when it comes to security, because we think it will not happen to us. In the perfect internet, privacy, security and convenience would all be optimized, but the internet is not perfect. Take an airport, for example: you can make the airport really secure, and have everybody go through a full body cavity search before they go on a plane, but it would not be too convenient. On the other hand, the airport can be all about privacy, without asking people who they are and just letting them go on, but clearly something would then happen in terms of security. What I chose to do is to start another path, which is an internet that is parallel to the one we have, based on convenience, because if you just want to check movie times you don't need to have security. However, at the same time I wanted to have something that is really really secure all the way, to the point of ensuring it, because if we don't do that, the future is bleak.

In 1967, every high school graduate knew that the next big thing was plastics. In 2016, they know that the next big thing is cyber security. It is the one area that keeps on growing, and we cannot defend unless we have the right bright minds helping us with it. At this point in the game, breaches are so common that we experience a "breach of the day". In 2010, we had roughly one big breach every year. However, cyber criminals began harnessing something called the Zeus malware, which can completely replay whatever you typed, and no matter if you put your DNA or fingerprint, or even an iris scan, because it could just replay the session. Since 2010 we have been experiencing breaches almost daily, and the good guys need an advantage in order to change the game on the bad guys.

A fake tweet published by AP, a news agency that said that there was an explosion at the White House, dropped the Dow Jones by 150 points in 90 seconds. The value of that was $136B. This is the largest heist in history, happened two years ago, and many of us are not aware of it. The hackers behind this were the Syrian Electronic Army, and since they knew that this tweet is about to come out, they shorted stocks, knowing that their value is going to go down, and made a lot of money from doing so. There is no anti money laundering (AML)

rules against it, this is completely legal, and if we don't stop this with greater authentication, we are going to fund a lot of bad things.

Twenty years ago, a caricature said "on the internet nobody knows you are a dog", and this is much the same today as well. The problem is that if we cannot identify exactly who is on the other end, the result can be disastrous. It can be a nuclear power plant, or billions of dollars can get lost by SWIFT, and it can be your medical records. We are fighting very creative and motivated people, not predictable systems. You can't change the equation just with software, or just by plugging something. The people on the other end are extremely motivated, because they make a lot of money if they are successful.

I want to discuss crime as a service, and specifically the Darknet. On the Darknet you can buy many different things, including passports and citizenship application documents, even for the USA. You can even buy crime online these days. If you're looking for a murderer, for example, there are different types and ranks of murder – regular, missing in action, death in an accident, etc. You can pay for that online, just like you shop at Amazon and eBay. The attack probability, on any one of you, is merely a function of the incentive. If you would have a website that sells straw hats, which no one cares about, no one would attack you; but if you sell something that could be changed on the street for $50, that would be really interesting.

When the good guys bring a new solution to the market, it has a shelf life, because this is an arms race. When new technologies come out they are extremely effective, and as a time goes by and fraudsters figure out what they do, and perhaps post how to fight it, the effectiveness goes down and continues to do so. As practitioners, a good advice would be to look at what Sun Tzu wrote in "the art of war", over 2,500 years ago: "if you know the enemy and know yourself, you need not fear the result of a hundred battles; if you know yourself but not the enemy, for every victory gained you will also suffer a defeat; if you know neither the enemy nor yourself, you will succumb in every battle".

Lastly, I want to talk about the price of shame. We all want to think we are secure. We want to say we are secure, but are we really? According to the Rockyou list of most common passwords, 18% of their users use the password 123456 to their accounts. This means that this password opens 18% of the doors. And there are other passwords on this list

that can give us access to many more. As security practitioners, we claim that we can't really guess passwords, because we have a limit of three before we are locked out, but why can't we just guess once on the entire list? In the UK, many people tend to pick their favorite soccer team as their passwords, which, again, is a problem. And for the price of shame: if you go outside your office and find a USB marked as confidential, would you be curious enough to see what was on it? When asked about it in person, many people would answer "no" or "maybe", and only a few would say "yes". However, in an anonymous survey online, people's truthful answers would be very different, and many would answer "yes".

At the end of the, day curiosity would kill the cat. We can put all the firewalls in the world, all the security measures, but if you pick that USB or do one thing that is insecure, you are risking everybody else with you.

For conclusion, here is a free tip. Mat Honan is a Wired reporter, somebody who really knows what he is doing when it comes to security, and still, his entire digital life was taken over because he picked the same passwords in all of his accounts. What you can do today is one thing, change your passwords, because if your passwords were just breached last night, you will just render them useless, right now. You don't need money, you don't need instructions, you already know how to do it. And as a good hygiene, change your passwords every month or every three months, because the only thing necessary for the triumph of evil is good men and women like you doing nothing.

WENDY NATHER, RESEARCH DIRECTOR, RETAIL CYBER INTELLIGENCE SHARING CENTER (R-CISC), USA

I came to talk about why we need to talk. I am going to discuss threat intelligence and threat intelligence sharing. We hear a lot about it, but part of this is the fact that it starts just as gossip. What typically happens is that somebody sits down with a beer with a friend in a pub, they sit together and someone says, "we have seen something very strange, is this something that you have seen too?" When I ask people if this is what they do; if they have peers in other organizations that they talk to, they say yes, and my next question is "does your management know?" to which the answer is "no", nobody knows about

this. What we are trying to do is take this from the level of gossip to grown-up threat intelligence sharing. This is not the military or the financial institutions; I work with retailers, which is quite a different sort of thing. I am going to tell you about what the real world is like in threat intelligence sharing.

First of all, one of the principles is that trust tends to happen between individuals, not between organizations, that is a problem that we have to work on. Secondly, the value of that threat intelligence depends, in part, on its being exclusive. If everybody knows it, it's not worth as much. That is a direct conflict with the utopian idea that we have that we are going to share everything in real-time, all the time, automatically. This is not the way it happens. Any time that something happens, an incident or personnel change in an organization, just like a signal changing to a default frequency, the sharing tends to default back to two people and e-mail. Even if they have a great threat intelligence platform, it always goes back to e-mail.

In 2015 we formed the retail ISAC, or the retail cyber intelligence sharing center. This was spun off from RILA in the USA, we got seed funding from about 30 top retailers, one of which is Target, and I have to say that at this point they have one of the most sophisticated threat intelligence operations that I have ever seen in the commercial sector. We currently have about 80 members, but also it isn't just typical retailers, anybody who is doing commercial services – automotive, fast food restaurants, hospitality, casinos, all sorts of organizations so it is a very big tent.

How do we do this, get people to share? We do social engineering. And let me stop here and say that I think the job of a CISO involves the biggest, hardest social engineering that there is, even more than that of a pentester – if you can get a thousand people to click on a link I am not impressed. If you can get a thousand people to stop clicking on a link, then I will be impressed. We have a lot of social engineering work to do to get these organizations to share with each other. One of the things we do is to emphasize the personal connection, to build that individual trust. We get people to work together face to face, to talk to one another, we introduce them individually, and so we keep bringing it back to the individual level to build that trust. We also have been known to use alcohol – if you get a nice dinner together with

people and a little bit of wine, people will talk about things that are going on that they will never ever put in writing.

This is another form of social engineering, and as pentesters and red teamers know, people like to be helpful, so we do have members who have joined our organizations because they want to help the community, and that is something we want to encourage. Going to someone and saying, "this organization needs help with this and we know you are an expert at it, would you be willing to talk to them?" has worked quite well.

Finally, we remind them that they have control over what they share. Anytime a member makes a submission to us, we say "we would like to send it to this group, which contains this type of people and organizations, is that all right? Can we use your name or can we not use your name? Did we sanitize this the way you wanted it?" We remind them over and over again that they have control, and that makes them more willing to share.

Another thing that we have come up with is the use of templates. Just listing the sort of things that you, as an organization, would want to share, so that you can get it signed off by your management one time, instead of having to go and ask permission every time you want them to contribute something. We have a relatively simple template, saying "this is the sort of information that we would share if we were reporting a phishing attack". It goes from mail headers and source domains and IPs, all the way down to the time range, which is very helpful for other members so they know where to look in their logs, and also what sort of tool found it, which is also very important, if it was your web filter, if it was picked up by Snort – that also helps them find the same sort of information. Attachments are difficult to share, unless you have a platform, because most organizations now have mail filters that strip malicious attachments, so you can't just share them that way. However, for all of these, there are some elements to the template that some organizations just won't share, so we might have to take out the target recipients, for example. But this is the conversation that we have to have over and over again with our membership to standardize the sharing that they are doing.

The other problem is with something like the traffic light protocol is the definition of an organization. Is an organization your company? Is

it the ISAC and all of its member organizations? What does it mean to you, and how comfortable are you to share with all the different parts of an organization? We have this problem all the time. In particular, we found out the hard way that a lot of our members did not want to share anything with the government. Certainly, there is a more adversarial relationship between the private sector and the public sector in the USA, they are very nervous about sharing. The other thing we didn't think about is that they also don't want to share with vendors, We have vendor members of our ISAC, but some are concerned, for example, that if they contribute threat intelligence, that the vendor will take it and commercialize it and make money off of it. They are very nervous about that.

Commercial interests in threat intelligence pose a great obstacle to sharing, and I can't blame the threat intelligence vendors for this, because this is part of their business model. However, they have Intellectual Property in the form of the threat intelligence, that they don't want to share unless you pay, and they may hold something under embargo for a long time; they may notify our members but say, "you cannot use the name that we have picked for this malware until we publish the report in two weeks' time," leaving us without a proper name to call the threat. There are also marketing and sales, and vendors are always going to want to approach our members and make sales. These are all things that work against the dynamics of sharing that we are trying to encourage.

David J. Bianco's Pyramid of Pain talks about what different indicators are shared in threat intelligence, and how painful it is for the adversary to change them, once they have been shared and exposed. Hashes, at the bottom of the pyramid, are extremely easy to change, and in fact there is so much customized malware today that there is no point in telling another member to look for the same hash, unless you are looking at a historical sample. They are not going to find the same hash in their environment. IP addresses are also easy, as well as domain names that are easy to predict. There are some vendors that are doing that, and proactively sinkholing them. This pyramid continues all the way up to who the actor is, and what their manual techniques and processes are. Those are very hard for them to change. Those things that are hard to change are the most painful for the attackers, and tend to be the most static.

Now let's flip this pyramid on its head, and look at what we can do as hunters with this information. What is static and what is dynamic? What tends to be static, which we can automate looking for, is all the legacy malware. The Conficker worm is still out there, and we have signatures for it. We can use automation to look for anything that is not under active development. But when it comes to malware under active development, we have to put more people to look for it, and then finally, when it comes down to engaging in real-time with the adversary, where they are reacting to what you are doing, you have to put a lot more people on that. That is going to be a very dynamic environment to work in.

Next we have unstructured threat intelligence. I know that everybody is very much in love with machine to machine sharing, but this is a very unstructured environment. The problem is that a lot of intelligence comes in the form of a message, "we had an attacker that was coming in with 700 attempts per day, as soon as they saw that we were on to them, they went low and slow, they ratcheted their attacks down to maybe seven per day, and they did not re-use a single IP until a month later." That sort of thing is very valuable intelligence, but it isn't structured. In my opinion some of the best intelligence comes in the form of a story; however, you cannot tell a story using XML. This is a major part of the threat intelligence sharing that we still need to adopt.

Other problems and complications of data sharing are that most are happy to share what they have blocked, unless they are incidents, and that they don't want reprisal from adversaries. But the most important point is that brand reputation is much more important to retailers than liability, so the Cybersecurity Information Sharing Act (CISA) in the USA, for example, which was a great idea, is not really helping. It is not making organizations more likely to share information. There is also the velvet rope problem; if you do not know the source of your intelligence, and you can't vet it and make sure they know what they are talking about, you will not want their threat intelligence. My retailers only want data from sources they can vet, they have enough data already that they need to prioritize.

When it comes to lessons learned from the cyber apocalypse, taken from the Department of Homeland Security's cyber exercise, we found that politics still plays a part, even (and especially) in an emergency, and government does not scale. Technology is not sufficient, especially

if you are sharing something widely – you probably watered it down so far that it isn't useful anymore. Finally, use any of these things: think about multiple communication channels; be careful and explicit about sharing restrictions; try templates, but use whatever works; when automating your process, don't forget the sharing stage. The bottom line is that it will come down to you and our contacts, which is another reason why you need to network as much as you can, and it is also another reason why we need to talk.

3ED SESSION: TERROR, ESPIONAGE AND CRIME

JOHN P. WATTERS, CHAIRMAN & CEO, ISIGHT PARTNERS A FIREEYE COMPANY

The topic that I am about to discuss is close to all of us in the cyber security industry – threats on the horizon the Internet of Things, operational technology, and what it might means to us. I am going to touch a little bit on the threat trajectories that we have seen around us, but more importantly, examine how we can put that in the context of risk, and use that risk framework as a way to resource our companies and our governments appropriately.

The days of spending countless dollars of cyber security funds because there is fear, uncertainty and doubt, are about to end soon, and people are going to have to make rational business decisions about why they invest in certain types of security programs – what is it they are trying to protect, what is the value of what they are trying to protect, and what does that value at risk mean for that organization if they do not effectively protect it. Basically, trying to move this from a security paradigm into a risk paradigm.

The most popular topic and trend of threats we are looking at today is crime. Crime has existed long as long as humans have exists, and cyber crime has now become a profound element that we have to live with as consumers, with all the hassle it involves; even if you don't have to pay your credit card bill when there is a false charge on it, you still have to go through the process of getting it renewed, and so on, and

so crime is a hassle to us as consumers, it is a risk to organizations, and it certainly makes it risky to trust our ecosystem.

The scale of cyber crime has grown from thefts of small amounts of money from a large number of customers – targeting credit card processors, credit card issuers, retailers merchants, online banks – to what we have seen of late, which is targeted attacks for large smash-and-grab operations, not unlike Bangladesh. The attackers are currently targeting commercial accounts rather than just individual consumer accounts, in order to get millions of dollars instead of merely thousands. The stakes really rise in terms of criminal activity, to try and get larger amounts of money in smaller-time operations, where they do all the reconnaissance work, all of the thoughts to try and understand where the holes are, and where are their vulnerabilities in their process, and then the attackers go in for large amounts of money. That is a real trend we have seen on the criminal side, which has moved up the impact to customers rather dramatically.

Another issue is espionage. Israel is a complete innovation hub for the world, one of the top tech centers in the world, and certainly a life-blood of the economy here. That is not lost on the rest of the world, which may be behind in terms of technology and innovation, and can spend much less money on R&D. Sometimes they prefer to hijack Intellectual Property, and use that to replicate businesses. We have seen this in the USA, and this has been happening more and more worldwide, including Israel. In terms of the Intellectual Property in the engine of economic growth, which is produced through that Intellectual Property, that is a real threat that you have to pay attention to as you protect your data, protect your Intellectual Property, and in essence, protect your economy both now and in the future.

Cyber terrorism today has been a lot of a concept move, but you haven't seen a lot of activity in that front, in terms of what is really causing serious consequences to our industry and to our governments. However, you have a convergence now that is taking place between motivation, intent, and capability. The motivation and intent are there, and the capability today is increasingly becoming merchandized in the underground market to a real capability. What might have been a very sophisticated criminal group or nationally affiliated entity is now able to be purchased and used by terrorist groups.

There is, however, a crossover between terrorist groups, criminal activity, national groups, and financial activity. Think of Bangladesh with an axis back in north Korea; the nation state targeting another bank in another country for financial gain. You also see nation states targeting commercial entities for damage, which can be called an act of terrorism, and certainly at least an act of vandalism. Then you think of what is going on in terms of terrorist organizations that use traditional criminal activity as a mechanism to fund physical terrorist activity. So how am I going to fund my activity as an island, when I am on an enclave, trying to fund myself for my operation, where the funding lines are getting more and more challenged? If I can conduct criminal activity to harvest money from the internet, then I can turn around and use that to fund physical terrorist activity.

The threat environment we are seeing is really converging. There is a lot of confusion on the who, what, why, where, and when, which really is a foundation of intelligence. Intelligence is a capability that enables decision advantage over the adversary: Who is behind it? How are they executing? And how do I understand their playbook to the extent that I can detect and defeat it efficiently and effectively?

Every enterprise, whether it is a commercial entity or a government, has a threat register, whether you know it or not. In your own ecosystem there are threat sources and threat methods targeting you and your environment, and you have a threat register that presents the real risk to your organization. That register contains the traditional hygiene threats, noise on your network that may not be targeting you, they are just indiscriminate threats; there are threats around your enterprise – a government agency in a certain country, a financial services entity, or an energy sector player, etc. – and you have to think of all of the threat register scenarios, and examine what are the actual impacts then of each of those threats.

Traditional risk equals threat times vulnerability times consequence. That has been lost on the cyber industry for many years, as people focused on technology and implementing people and process to be compliant with the rules. There is a lot of talk about the threat side, but there hasn't been mapping of threats to impact, and investments in security programs to mitigate and avoid the impact. Now, let's start putting it in a framework.

You create a threat register, with all the threats that matter to your enterprise, and examine what are the real consequences you are trying to manage with your security programs, and map it to an impact – which threats have serious consequences and which ones do not. Then evaluate your entire program span in light of that residual risk; you got threats, the impacts are going to drive how you are going to prioritize your investments, and what you are left with, you invest in countermeasure programs, security programs, to reduce the probability of those threats. You can get very precise and granular in the way you begin to lock your resourcing plans against your threat reality, in a way that can continuously adapt over time, as your threat reality changes.

Building an intelligence-lead approach to security, and in fact a cyber risk management structure around security, requires an understanding of your threat environment, building collection requirements and intelligence programs, which can deliver intelligence against that threat environment, so you understand how it is changing. You have to understand the impacts – business impacts, brand impacts, disruptive impacts – to your business and enterprise, and how to protect yourself over time as these threats change. Fundamentally, as you think about the threats today, people are beginning to think, "what are the consequences of threats to my organization? What are the real impacts?" Then, when you look at your investment program and your security initiatives, how do those map to one another?

I would challenge you to begin building a really tight mapping of the investment decisions that stand in front of you, with the initiatives that you are going to fund, the threats you are trying to mitigate, and the impacts. You can find simple ROI on security, where you spend $1M to avoid a $20M problem, or you can invest $100K to tackle a $10M problem, but don't invest $10M to avoid a $100K problem. You have to really understand the impacts of the threats you are investing against, and I think that will go a long way towards driving precision and efficiency in your investment strategy, and create a communication system between you and the executives, where they understand what you are talking about.

There has been a huge security communication chasm between security organizations and executive leadership in the boards, because many of the security executives the industry say things like "we blocked 40 million malware infections last month", but there is no context of

what that means. Is that a big deal? Not a big deal? Should you block 50 million, or maybe 5 million? The numbers really don't make any sense from the executive perspective. When you say "we invested these dollars in this program, and the threats we were able to detect in the last month had consequences that were significantly higher than the amount that we invested", it means that we invested $1M in our security initiatives, and through these people, process, technology, and intelligence, we were able to detect that the threat was activated against us, defeat and remediate it, and therefore we were able to avoid a $10M issue for $1M of investment. That is a security executive that will transition upwardly in their executive suite as a cyber risk officer.

You have even seen some of the titles change from CISO to Chief Information Risk Officer, it is really a natural progression, and much of the turnover we have seen in the security industry – particularly among CISOs in the USA, it is about sixteen months as the average tenure – I think will extend materially as CISOs can begin to become business partners, and line up in a rational risk framework that their investments are going to purposely mitigate risk. As you think through the threats, look at how your investments map to those threats, and how those impacts are mitigated with those investments.

DR. KENNETH GEERS, CYBER CENTRE AMBASSADOR, NATO

I am not a technical guy, I have a background in international relations. I started my career in government some time ago as a linguist and intelligence analyst, and in the mid-1990s, in the middle of Maryland, where I worked as an analyst, there was a pressure for a geopolitical analyst to know more about C2C, computer to computer communications, as well as human activities. I transitioned, and by the end of the 1990s I was working as an intelligence analyst, but on cyber things and computer affairs. I worked at NCIS and NATO in Estonia during the cyber attack on Estonia in 2007; the pentagon asked me to move there to help build the cyber center, which currently has twenty member nations.

Now I live in Ukraine, and for the past year I have been following cyber attacks for NATO. I edited a volume with twenty authors looking at the cyber dimension of the conflict in Ukraine, and we found a trend here: basically, every stone you turned over, there were attacks and

operations, none of them decisive, none of them extremely violent or flashy, and yet, if you are in charge of an organization, no matter what kind, it seems like today cyber security is going to be an element that you are going to have to worry about. For example, in Ukrainian politics, the election was thoroughly hacked. Communications of diplomats were stolen, uploaded to YouTube and announced on twitter. In social media, accounts popped up, criticized the government and then disappeared, and when you searched on that person they didn't really exist. In the military space, there were special forces operations in eastern Ukraine to isolate Crimea and eastern Ukraine from Kiev, and so on. Every sector was hurt; for example, in the business sector, smart TVs were hacked with Russian propaganda.

There are many more examples of cyber attacks, and one of the takeaways is to simply use common sense and logic, current events, and geopolitical background, when you think about what you are seeing. I spent long hours in the basement of the pentagon, looking at long lists of IP addresses to which data was flowing from the pentagon for years, but then, from a law enforcement counter-intelligence perspective, all you really know is that you are losing data, and that it is going to what is called the "first hop". The problem with the first hop is that you have an IP address, and that is it, really. You have to dig deeper in terms of traditional investigative powers and abilities. For example, in 2007, when Estonia was under cyber attack, the vast majority of the packets were coming from the USA, and it certainly wasn't the USA government that was attacking Estonia. Then, when those packets began to be filtered, the attacks came from Egypt, and then from Vietnam. It is a global architecture.

When I was an analyst at FireEye I wrote a paper after looking at 30 million malware communications over an 18-months period. The USA appeared there as a source for malware communications, as well as any other country; it is a global space, that is all tied together, and malware communications between nations is an international space, which is bigger than any jurisdiction and any sovereignty on the planet. This is the challenge that Russia and Iran and North Korea have now, which leads them to fear the internet while they are trying to use it for political and social control. Another disturbing factor here is that there are malware connections between any two countries on the planet.

This means that if you are a hacker or an intelligence operative, you can route your communications in a different way every time.

When I wrote this report, I discovered all kinds of new diagraphs for example, .ax is the top-level domain for the Åland Islands, a small sovereign island between Finland and Sweden, which I didn't even know existed. Unsurprisingly, Åland has its share of malware servers, like every other city state, enterprise and of course country on the planet, but from a law enforcement and a counter-intelligence perspective, this creates enormous headaches. As an investigator, how are you going to follow this trail back? At the very least, to me it seems like you have to be a nation, because for anything short of that, true attribution is hardly possible, because you need to pull together signals, intelligence, diplomacy, law enforcement, and all kinds of larger tools and tactics in order to get there, otherwise you are left with this problem of the first hop.

Unfortunately, many malware servers are located in places where there is a lot of infrastructure, such as the USA. However, this also gives places like the USA an advantage from the standpoint of oversight and monitoring. You want to have more data to look at, the more data the better, so in this sense I would even suggest that the USA has a certain strategic depth in cyber space, which Napoleon and Hitler found Russia possessed in traditional geopolitical space: when they tried to invade Russia, they discovered that it gets very cold there in winter. In the same way, the USA has many vulnerabilities and many targets, but at the same time it would be very hard to wipe the USA off the internet, due to its overwhelming size, whereas a country like North Korea – and I would suspect that even countries like Russia and Iran – have to worry about that, because the more authoritarian you are, perhaps the fewer internet connections you will have. You may not know this, but Antarctica has more internet connections than about a third of the UN members, and while those are for research purposes, it also gives you an idea of just how some countries fear internet connectivity.

There are plenty of recent cyber attacks, which let you know that it is a problem not only for every institution, but that the line between network security and national security is hardly there anymore. For instance, Bruce Schneier said about the OPM hack in the USA, that it may have been a cyber Pearl Harbor. Why would he say that? I think

it is because the intelligence haul from this attack is so large, it is hard to get your mind around it. For example, all the people who work in the USA government, their polygraphs, as well as all of the things they have told investigators, their financial status, and so on – all was taken by a foreign government. This puts them all in jeopardy of being manipulated and targeted very specifically.

Over time, targeting has become very specific; in the past, a computer would be in a room, and you would have to break into that room, but now we all have super-computers in our pockets, which is cool, but at the same time it allows for very simple targeting. For instance, in Maidan, Ukraine, where the protestors were moving around the city, the government was able to target them depending on what street they were on, or if they were close to the presidential palace. You can achieve targeting in numerous ways, but the fact that you are closely connected to the internet on an intimate, personal level – for instance, through social media, a trusted circle that you have self-selected out of the whole world – means that intelligence agencies, information and operation folks, propagandists, politicians, can target you personally, and that is a very disturbing factor.

Yesterday I saw a cartoon on the internet, where a guy was walking through a shopping center, and he sees various advertisements that are targeting him personally. That is possible to do, to find out about things he likes to eat and things he needs. This shows you how tailored things including information operations can be. When you look at economic attacks, this could also easily be a military intelligence operation to move money. when even money has been digitized, and you can move it around the world at light speed. Everybody is short on budgets, and the fact is that in cyber space today there is very little fear of retaliation and prosecution, and so it is very possible that even militaries might resort to this kind of activity.

Finally, in western Ukraine there was an attack on a power grid, which everybody was waiting for to see when it would happen. We know that the connectivity is there and the vulnerability is there to manipulate critical infrastructure, but intelligence agencies and militaries do a lot of experimentation and signaling in cyber space, because they are trying to figure out where are the red lines, in terms of what you can and can't do. I would suggest that the part of the malicious activity in cyber space today that is done by militaries is a little bigger than we

realize. This is because if you are in charge of making sure the next Pearl Harbor doesn't happen, or if you are in charge of making sure that you can win a war against your adversary, there has to be a lot of hacking happening during peace time in order to be ready for war.

A big difference between a traditional military operation and a cyber operation is that you can choose to do a traditional military operation today, and you could send soldiers across the border – a spy or a tank or a plane – but hacking takes a long time, it takes months, maybe years of painstaking subversion to get into Microsoft or Google or into the power grid that guards Paris or Washington or Moscow. What this means, unfortunately for military organizations, is that they look much more like a covert arm of the government, because packages don't wear uniforms. A particular unit of the military is going to be tasked with doing things that look a lot more like a covert operation in peace time.

I am also on such a cyber command academic team, and I know that many technical personnel hate the phrase "cyber Pearl Harbor", but in fact, we spend a lot of time there talking about cyber Pearl Harbor. The challenge here is that because computers and processors and hard drives sit on planes, tanks, and ships. They are floating or flying computers, which means that "terminator" scenarios are much closer than we think. You are going to have to give some of these attack vehicles code that gives them autonomy, so that they know whom to kill and when, because they might be too far away for traditional hands on control. But the encryption, the source code that sits on these machines is always vulnerable to some kind of attack.

The players in cyber space is also an area of concern, because there is so much plausible deniability in cyber space, so much anonymity, that the question of who is attacking you is a challenge. You could always pass it off to outsourced contractors or route it through countries with which your target has poor law enforcement or diplomatic relations, so it makes it very difficult to trace it back. In addition, when the hacking team, for example, has so much hacker expertise within it, then it gives them the ability to do things that you might think that only governments are capable of.

We are not on a leveled playfield around the world, there are some very open and transparent countries, and there are some very authoritarian

and very shortsighted countries, all within the cyber space. For example, when Putin talks about national security, I really think what he is talking about is regime security, and there is a very big difference between the two. Likewise, when the cyber negotiations take place between east and west, sometimes one group is talking about cyber security and the other is talking about information security. Those are two different things, because then a blog that criticizes the president would be seen as a cyber attack.

There are only three kinds of basic cyber attacks: stealing information, blocking information, and changing information. All of these things will be done in a military context, however, because of the nature of hacking and the time and the energy it takes to do it, you have got to get started now.

YOSEF LEHRMAN, DIRECTOR OF INFORMATION SECURITY, NEW YORK CITY POLICE DEPARTMENT

Everyone knows that the New York city Police Department is the largest municipal police department in the USA; we have approximately 50,000 personnel overall. New York city is a major financial and geopolitical nerve center of the world, with over eight million people to protect and serve. With such a large population, it is vital that we have computer systems that are available when we need them, that we have data that we can trust to make sound tactical decisions, and of course, that we prevent unauthorized individuals from accessing that data. Today I would like to share with you some thoughts on cyber terrorism: what it is, what it isn't, how we can detect it, and most importantly – how we can defend ourselves against it.

One of the major sources of frustration, and probably the only point of agreement among academics, politicians, and security professionals, is the lack of a clear and unanimously accepted definition of the term "terrorism", which has consequentially had a negative impact on attempts to create a common terminology for cyber terrorism. Without the ability to appropriately define terrorism, we cannot begin to have a clear and coherent discussion of what the cyber version of terrorism is, which has led to the term being applied to a wide variety of cyber threats and attacks.

If we begin with the assumption that cyber terrorism is the employment of terrorism in cyber space, then it follows that in order to be considered an act of cyber terrorism, first of all the act must sufficiently destructive or disruptive to generate fear comparable to physical acts of terror. Second, the perpetrator or perpetrators of the action must not be nation state actors, as actions by nation state would most likely fall into the category of cyber war and not cyber terror. Third, the intensive goals must be political or social in nature. The definition set forth by Kenneth Hima, in his 2007 book *Internet Security: Hacking, Counterhacking, and Society*, meets all of these criteria; by this definition, cyber terrorism is highly damaging computer-based attacks or threats of attack by non-state actors against information systems, when conducted to intimidate or coerce governments or societies in pursuit of goals that are political or social. Under this definition, actions taken by non-state actives to date would most likely not be considered cyber terrorism.

The most destructive or disruptive attacks have not had political or social goals, the goals have typically been economic. The attacks with political or social goals have generally not been intimidating, but rather simple web defacements, twitter compromises, things of that nature that have been disruptive, annoying, but have not had much impact. This doesn't mean to imply that cyber terrorism is not an area of concern; on the contrary. We are seeing terrorist groups that are becoming quite skilled at using cyber space to facilitate their operation in many ways. A number of terrorist groups have advocated conducting cyber attacks, and some have even engaged in some light hacking. Additionally, new hacking groups have emerged, which, while allegedly are unaffiliated with terrorist organizations, there are definitely some unofficial connections between them.

The available evidence to date does not support an imminent threat of cyber terrorism. We have seen some nation state actors that appear to have taken an interest in cyber attacks on critical infrastructure; however, there have been few indications that terrorist groups that are backed by these nation states have taken up the same interest. Terrorist groups unaffiliated with nation states have also apparently not devoted much discussion to this idea, at least compared with discussion and research on traditional attacks. One possibility, which has been raised in the media as well, is the concept of cyber terrorism being used in conjunction with a physical attack, perhaps as a means of

amplifying the effect of physical attack by either impeding emergency response to the incident and/or to increasing fear.

However, traditionally, terrorists have not integrated multiple modes of attack. Even in attacks that have involved multiple coordinated attacks, such as the recent bombing in Brussels, Belgium, what you have seen is multiple occurrences of the same mechanism of attack, and less multiple modes of attack within a single incident. It is unlikely that terrorists would suddenly succeed with an attack requiring coordination across the cyber and physical domains, without training, discussion, and planning, actions that would hopefully be detected by global intelligence agencies. Discussions around online training and cyber attack methodology and techniques have tended to skew more towards ensuring operational security for terror group members, and less towards actual attacks of consequence.

As an example, media publications released by the Islamic state typically offer concrete operational guidance. The most recent issue of Dar Al Islam, which is the French language magazine of the Islamic State, contained a fourteen-page technical section. This was not a hackers' manual on how to launch successful attacks, and it did not provide detailed guidance on how to attack high value critical infrastructure, rather the section was dedicated to ways in which one may operate online anonymously. Another illustrative example is the video that was released by Al-Qaeda in June, 2011. The video was called Al-Qaeda Al-Shabab Video on E-Jihad – The Internet, and it shows imagery of high-level attacks, and people working with computers doing all sorts of very technical things. There are books about hacking in the background, but the video itself advocates low-level denial of service attacks, harnessing computers to target another website and to make that website unavailable online. Again, this is annoying and disruptive, but websites of large corporations, such as the ones advocated in the videos – CNN, Yahoo, Amazon – have typically proven to be very resilient to this sort of attack, and while I don't minimize the economic damage that would result from taking these sites offline, I don't think it would rise to the level of cyber terrorism, at least based on the definition that we have put forth until now.

A greater concern than a terrorist group developing the capability to launch a successful terrorist attack is that of terrorist organizations forming an alliance with hacker groups. There are thousands of

hacking groups worldwide, and in any moment a group can align itself with terrorists, adding to their skill base and apply it to cyber terrorism. The idea of terrorist organizations aligning themselves with traditional criminal elements is not unprecedented, there are many documented cases; for example, smuggling or other criminal activities that have been used in support of terrorism. While the vast majority of hackers would not support terrorism directly, and most likely would not condone loss of life, nevertheless it is likely that at least some of them would hack in support of the same objectives. We have seen this with Anonymous, for example, where Anonymous Op Israel actually supports the same stated objectives as many terrorist organizations, and yet Anonymous also has an Op Isis operation, which is allegedly against terrorism. There have also been numerous examples of terrorist organizations utilizing the internet to distribute documents, videos and/or audio recordings to recruit and spread propaganda.

There have also been examples of terrorist sympathizers using the internet to compromise information, to steal information that can then be used to heighten people's sense of fear; distributing public information, and making personal identifiable information public. The most significant threat, though, stems from lone-wolf style actors with specialized knowledge and cyber capabilities. These actors could be selected from known terrorist recruits, or more concerningly, radicalized from the general population.

Of particular interest is the case of Ali Saleh Kahlah al-Marri ,a Qatari citizen who was arrested shortly after 9/11 in the USA and allegedly, at least in the media ,has been linked to an objective of conducting cyber attacks on USA banks .Allegedly ,this individual was placed into the united states by Al-Qaeda for the sole purpose of conducting cyber attacks on USA banks .He was arrested in ,2001 and after much legal wriggling he was eventually sentenced to time served and was released ,and he is now back in Qatar ,presumably .However ,what makes his case particularly concerning is that he was sent to the USA for the sole purpose of going to graduate school to gain a degree in computer science ,and then use that knowledge against the USA itself. If this trend is going to continue ,this poses a very serious problem to the national security of not only the USA ,but of any country where you have people who have learned all the techniques ,tools ,and tricks of

how to hack ,and can now use them against the critical infrastructure of that country themselves.

Fortunately ,ultimately in regards to securing our networks ,the same basic principles apply ,irrespective of the attacker's origin, methodology or ideology .To start with ,I am going to say something that everybody hears all the time ,that system appropriate system hygiene is vital .According to the Center for Internet Security ,if an inventory of authorized devices and software is being maintained ,secure configurations for all devices appropriately developed and managed, continuous vulnerability assessment and remediation conducted ,and administrative privileges actively managed and controlled ,approximately 80%of the attacks could be prevented.

Obviously ,there are other measures that can be implemented to prevent intrusions from occurring or to mitigate the impacts of those intrusions; for example ,application whitelisting and network segmentation .Taken together ,if properly implemented ,we can probably prevent 90% of the attacks ,and maybe even more .However ,despite the best of efforts of security professionals ,it is impossible to completely prevent attacks. As such ,organizations must develop a plan to address the inevitable cyber attacks before they occur .This plan will be most effective when developed by a working group ,headed by a strong leader and made up of a cross-functional collection of senior managers .The objective would be to map out a risk profile for the organization and identify possible attack methodologies ,targets ,vulnerabilities ,and impacts .It is important not to get stuck trying to come up with detailed estimates of damage ,an estimate that most likely won't be highly accurate in the event of a real-world incident in any case .Instead, rough estimates are acceptable ,just enough to provide a sense of scale and the type of potential harm ,which should then be used to develop a risk mitigation strategy .When creating the working group to develop the organizational risk profile ,there is often a struggle to determine where within the organization the group should fall .It is absolutely critical that the group reside within the technology area of the organization.

Cyber is often considered within the context of a variety of other fields –counter-terrorism ,espionage ,crime and so on – however ,cyber does not lend itself effectively to such stove piping .The fact is that cyber often bleeds between these disciplines as well as others ;it is a

technical discipline ,and oddly enough ,for some reason which I have not yet been able to figure out ,this particular fact is often overlooked. The OODA loop is a theory developed by USA military strategist Air Force colonel John Richard Boyd ,and the key concept here is that the loop represents the decision cycle ,or the process by which an entity reacts to an event :observe ,orient ,decide ,act .The theory posits that the key to victory is to be able to create situations where one can make appropriate decisions more quickly than the adversary ;in other words ,to close or shrink the OODA loop.

In the cyber arena ,the same tools ,tactics ,and procedures can be used either offensively or defensively .Most organizations have no problem placing these defensive tools ,tactics ,and procedures in the technology group .Therefore ,it would make sense to have the people who handle these tools ,tactics ,and procedures on the defensive side handle them in the offensive level as well .When an organization chooses to break this apart and to situate their intelligence – their observe and orient areas – within the intelligence component ,they decide within the executive component and act within the technical component ;not having these areas combined and working together, what they have effectively done is to enlarge their OODA loop ,and essentially all but ensured that the adversary will be successful .I am not advocating that intelligence be disbanded ,or that we should get rid of everybody except technical people ,my key point is that everyone needs to work together not only in the same organization ,but ideally in the same room in the same group.

I want to end on a slightly more optimistic note :the threat of cyber terrorism is not as high as you might think from reading some news articles ,but it is not nonexistent ,and will probably grow .In the event that terrorist groups begin to move towards conducting operations in cyber space ,there are some indicators that we should see .The first is execution of cyber attacks ,which means all sorts of computer network attack ,actions taken to disrupt ,deny ,degrade or destroy information or the information systems that the information resides within .That is not specifically limited to cyber terrorism .The second is acquisition and distribution of cyber weapons ,R&D in cyber weapons ,and training in the use of cyber weapons .The third is discussions about declaration of intent to perform and/or calls for performing cyber attacks .The fourth is pursuit of formal education in information technology .The

fifth is incorporating general use of the internet for communications and distribution of news and propaganda .The good news is that by appropriately framing the problem ,and appropriately structuring our organizations ,we are in an excellent position to successfully meet and defeat this threat.

DR. MADAN M. OBEROI, DIRECTOR, CYBER INNOVATION AND OUTREACH, INTERPOL

Before starting my presentation, I normally like to clarify the role of Interpol. Most people know what Interpol does based out of information coming from Hollywood. For me, it is my duty to clarify what we don't do. First of all, we do not have any secret bases around the world; our agents do not carry any guns; we do not do any car chases; and on top of that, we don't even do investigations. What do we do, then? That is what I will try to attempt to answer here. I will start with a very high level overview of what trends we are seeing in cyber crime, continue with the issue of challenges or strategic questions that law enforcement agencies are facing with regard to investigation of cyber crimes, and then I will propose an approach such as the one Interpol is adopting, and explain how we are utilizing that approach.

In regards to cyber crime trends, what we are broadly looking at is an increase in terms of ransomware; cyber crimes involving business e-mail compromise; attacks on the financial sector, including large scale attacks on international bank transfers, DD4BC that is distributed denial of service attacks for Bitcoins, and ATM malwares being deployed; increasing use of Darknet; increasing use of Crypto Currencies, including Bitcoins; Crime-as-a-Service (CaaS) being developed as a business model; and a large scale shift to mobile platforms.

When referring to ransomware we are seeing it evolving from normal encrypting devices to infrastructures, like hospitals being attacked. In terms of criminal use of Darknet, we see a large scale illicit trade and weapons. National identity documents like passports, utility bills, and national I-cards. Others use the Darknet for trading drugs. We also see large scale use of Crypto Currencies by criminals, not only for cyber crime, but also for some of the traditional crimes. We have seen cases of kidnapping for ransom, where the ransom has been demanded in Bitcoins. We are witnessing development of the

Crime-as-a-Service model, with various sites openly advertising their services on Darknet, and providing kits for ransomware and other hacking services, including hosting a marketplace for trading in secret information.

We are also seeing new forms of crime, such as: Bitcoin thefts; thefts of computational resources for Bitcoin mining; embezzlement by Bitcoin exchanges; market place exit scams; new forms of extortion, like sextortions and ransomware; and development of crime as a business model.

How do these changes affect law enforcement agencies? When we investigate crimes, there are major questions that are coming to the minds of law enforcement, and which are troubling us. The first and foremost question which we debate, and it has been discussed very widely, is related to ownership of data on the internet. It becomes very significant for law enforcement agencies, because it determines also in terms of whom should we ask for investigation-related information, and related issues.

The second question is in terms of large number of rules, regulations, and legal provisions coming into the picture from national governments – how do we enforce them, and if we can enforce them, what are the best points for enforcement? A case in point would be Crypto Currencies or Bitcoins, some of the jurisdictions have banned Bitcoin transactions. But the question is, how do we enforce these bans, and how do we regulate Bitcoins? Probably the only place point where Bitcoin or Crypto Currency transactions can be regulated is the point of exchange between Crypto Currencies and Fiat currencies, so we need to select our points of enforcement.

The third question is, who is capable of enforcing laws and regulations? Is it the state, or typically the law enforcement agencies, or is it some new actors, notably private sector, who are in the best position to enforce these laws? If that is the case, how does it impact in terms of investigation of crimes?

The fourth question is, who has the information and expertise? In law enforcement agencies, we very clearly believe that, as far as investigation in cyber space is concerned, both the information and expertise lie outside the domain of law enforcement, so we have no option but to work with other stakeholders.

The next question or issue is third party policing. This is one of the very debatable issues that have come up, because if you look at the statistics around the world, and compare the number or crimes happening in cyber space and the number of crimes that have been taken up for investigation by law enforcement agencies, there is a wide discrepancy. Not many victims report the crimes to law enforcement agencies, probably because they don't see much value coming out of them, in terms of what can law enforcement agencies provide. In this scenario, we see many third party agencies coming up, who do the investigations for these victims, but the question is: do they have the mandate to bring consequences on the culprits? And if not, how does it help the overall criminal justice system?

The next issue is very interesting, it is about the trust deficit. Here I would like to illustrate a recent event. I was at a conference organized by one of our partners, and where the partner agency was showcasing private-public partnership, how his company was working with Interpol to combat cyber crime. During the host's lecture, he started mentioning how they do not comply with all the directions of law enforcement agencies. How it is important for them to use discretion in accepting the request of law enforcement agencies .I have spent around25 years in police service ,and my mind went back a few decades ;there was a time when private companies would make a point to illustrate how they are compliant with laws ,and how they help law enforcement agencies in maintaining security and other notions .Now we see a trend where companies feel necessity to distance themselves from the efforts of law enforcement agencies .Therefore ,the question that came to my mind is :what has happened in between?

Clearly ,the answer is that we ,as law enforcement agencies ,and as I state in a more broader sense ,have lost the trust somewhere. There is a need to fill that trust deficit ,and that is what we need to work on .There are different reasons which have been given for this, I won't go into those debatable issues ,but the outcome is that there is a trust deficit.

Yet another issue that comes to mind is disruption versus prosecution-based approach .These days we hear more about takedowns ,how many sites have been taken ,down how many botnets have been taken down ,and less about how many people have been arrested ,charged, and taken for prosecution .Probably due to the disruption based

approach we are targeting the infrastructure of criminals rather than the criminals themselves ,which is the basis of prosecution-based approach .Clearly ,our disruption-based approach is less effective than a prosecution-based approach .However ,many times it is the only option available to law enforcement in absence of clear attribution, so we need to work on this.

Additional issues are related to attributions ,not only to technology –there is more which has to be done at internet governance bodies like ICANN ,and these issues need to be addressed .In light of these questions ,there is a clear need for recalibration of strategy by law enforcement agencies .Interpol advocates a multi-stakeholder approach to work with the private sector ,academia ,research bodies, other governmental organizations ,and communities at large .In this sense ,we advocate a four-action pillar approach :providing actionable intelligence to law enforcement agencies for concerted action ;building operational capabilities of law enforcement agencies in terms of skills infrastructures and SOPs ;providing research and strategy support to law enforcement agencies ;and working at a platform for international coordination.

Interpol and the World Economic Forum developed a model at Davos, that deals with how public sector and private sector can be used for developing actionable intelligence .It contains things that are good on paper :we should have a multi-jurisdictional and a multi-stakeholder platform .But ,how does it actually work in practice ?We have established a cyber fusion center where we embedded the sources from different law enforcement agencies ,academia ,various companies like Barclays, Kaspersky ,Trend Micro ,Cyber Defense Institute ,NEC ,SECOM ,and others ,embedding their physical resources in terms of manpower in our cyber fusion center which work jointly with our team to identify actionable intelligence for taking up with law enforcement agencies.

One example is the SIMDA Botnet takedown ,which happened in ,2015where we worked with Trend Micro ,Kaspersky ,Cyber Defense Institute ,and Microsoft .Law enforcement agencies from USA ,Russia, the Netherlands ,Luxemburg ,Poland ,and Singapore worked together for this takedown .Similarly ,if you look at the recent bank heist at Bangladesh ,where81$ M were stolen ,there we are working with Bangladesh criminal investigation department) CID ,(the FBI ,and Cyber Defense Institute .Other actors working in this area are FireEye,

BAE ,Symantec ,SWIFT ,Bangladesh Bank ,and we are working towards involving all the actors ,so that we can jointly form a task force to combat this kind of crime.

In terms of capacity strengthening ,we have various programs .One of our notable achievement was last year's development of a simulation-based Darknet and Crypto Currency training ,where we developed an in-lab Darknet and an in-lab Crypto Currency environment ,and this was done jointly with a Netherlands-based research organization known as TNO ,as well as SECOM ,which is a Japanese company .In order to train law enforcement agencies ,we also developed a digital security challenge ,where a cyber crimes 'scenario was created ,and teams from different countries participated and competed .This was, again ,developed jointly with NEC and Cyber Defense Institute.

Under research and innovation efforts ,we have developed forensic tools to trace Crypto Currencies and transactions ,and perform analytics on them .These tools have been developed by Interpol's cyber research lab jointly with SECOM .Last year we made a presentation at Black Hat ,where we identified a major vulnerability in Blockchain .This was, again ,done jointly with Kaspersky – the research happened in the cyber research lab of Interpol with resources embedded from Kaspersky.

There are different research activities that are happening ,and we are doing a large number of research projects in collaboration with Georgetown University ,University of Waikato in New Zealand ,University of South Australia ,IIIT in New Delhi ,as well as NEC .What we are saying is ,basically ,that there is a need for all stakeholders to come together to combat cyber crime ,and this multi-stakeholder also has to be a multi-jurisdictional approach .In Interpol's view ,that is the way forward to combat cyber crime.

4TH SESSION: HACKABLE HUMANS

PROF. NATHAN INTRATOR, RESEARCHER, BLAVATNIK INTERDISCIPLINARY CYBER RESEARCH CENTER, PROFESSOR, SCHOOL OF COMPUTER SCIENCE, TEL AVIV UNIVERSITY

The information in this article is potentially the most important one, because we want to hack the real brain, the real computer. I will try to explain why we need to hack the brain, and what does it mean to hack the brain. First, we need to be able to listen to the brain. A good example of why we want to do that is the F-35, Israel's new fighter jet, which costs about $200M. It has a very wide bandwidth data connection to the ground in real-time, so everything in this airplane is being monitored, everything in it, like pressure, for example, is being monitored. However, the one thing that is not being monitored is the pilot's brain, and you can imagine how important it is to monitor the pilot's brain. This is only one reason for monitoring the brain.

Before we go into the brain, let's go back a little bit in history and see how we monitored things in the past. About 60 years ago, the first wearable computer was invented – the first pacemaker. It wasn't exactly portable like today's computers, but it definitely extended the life of the person to whom it was connected. Jumping very quickly 60 years forward, Medtronic introduced their new pacemaker, an amazing computer with a 5-year battery. In addition to the cardiac activity it measures fluid in the lungs, as well as other parameters that we won't go into, and it can also function as a defibrillator.

The last thing I wanted to mention before moving on to the brain is monitoring stress, because obviously, stress is the key issue. One way to monitor stress, again not very successfully, is a lie detector. This is why lie detectors are still not accepted in court, because trying to interpret the stress coming from the brain through what is called the sympathetic system – which is the system which responds to stress and increases heart rate and makes the vessels tighter, and so on – is obviously not working so well.

Now, let's go back to the brain and to our fighter jet. Nowadays, we are still trying to find ways to monitor the brain. For that cause, we founded a company and developed a technology in the university,

which can read the brain only using two frontal electrodes, instead of dozens of electrodes connected to the entire surface of the head. By reading the brain through these frontal electrodes, we can actually tell a lot about what happens in the brain. There are also new sensing technologies, very flat electronics. One of the companies that develop that is MC10 in Boston, and they will have a little patch on the forehead that can actually do the brain monitoring. Of course, the key is not just the sensor, but the algorithms behind it, and this is what we have developed – algorithms that can take the information from two electrodes, and extract a lot of brain activity information out of there, using very advanced signal processing.

After we've covered the monitoring part, we move into hacking the brain itself. In 2014, prof. Itzhak Fried, who is one of the professors at Tel Aviv university and UCLA, performed a brain surgery on this woman while she was playing the violin. This was done in order to be absolutely sure that he was not removing her ability to play the violin, but instead curing a condition that harmed her ability to play the violin, which was a very close call. For this, he had to keep the patient awake and even playing, in order to pinpoint where he had to go.

A technology that is currently becoming more and more available is magnetic stimulation, which – unlike brain operations – is non-invasive, something that happens outside of the brain. This is where this technology is headed, it may be either magnetic direct current (DC) or alternating current (AC), and all these stimulations are now being thoroughly studied to actually stimulate the brain. So far, there has been some success; maybe this is a little premature to talk about all this at this point, but there are many studies, and some progress has already been demonstrated.

I envision that in the future, people will have a stick on the forehead and a couple of electrodes somewhere on their head, to perform the stimulation that they need; everything will be connected to the internet with a computer that is going to be small, because we don't want to carry a large battery; and that computer can be hackable. Suddenly a hacker will not be able to just get into our computer or into a database on the Cloud and obtain information, but will actually be able to get into our brain and even affect it. This is where we are going to, these are the challenges for this generation of computer scientists, and this is what we are dealing with.

DR. MARIE MOE, RESEARCH SCIENTIST, SINTEF; ASSOCIATE PROFESSOR, NTNU

I am a security researcher, and I am a patient. Every single beat of my heart is generated by a medical device, a pacemaker implanted in my body. Four years ago, I woke up lying on the floor; it turns out I had fallen because my heart had taken a break, long enough to cause unconsciousness. To keep my pulse up, and to stop my heart from taking breaks, I needed to get a pacemaker implanted in my chest. This little device monitors each heartbeat and sends a small electrical signal directly to my heart via an electrode to keep it beating. While the device helps your heart maintain its rhythm, it also stores information about your heart that can be retrieved by your doctor to program the device. But how can I trust my heart when it is running on proprietary code and there is no transparency?

When I got the pacemaker, it was an emergency procedure. I needed the device to stay alive, so there really was no option to not have the implant. However, it was time to ask questions. To the surprise of my doctors, I started asking questions about potential security vulnerabilities in the software running on the pacemaker, and the possibilities of hacking this life-critical device. The answers were unsatisfying. My healthcare providers could not answer my technical questions about computer security, and many of them haven't even told about the fact that this machine inside of me is running code, and there was little technical information available from the manufacturers of the device. This is why I decided to seek out this information myself, and started a hacking project. Imagine that your heartbeat is being controlled by a machine that is running code inside of your body. Wouldn't you also like to know if it can be trusted?

I did some research, and found the technical manual of my pacemaker after I had it implanted, and I was surprised to find out that it had two different wireless communication interfaces. One is near field communication interface that is used to program the device – after I got the implant, some settings had to be adjusted to work with my condition and my body; and then there is another, longer range communication interface, which can be used for home monitoring or telemetry, meaning that if you have this home-monitoring unit, in your bedroom, for instance, it will connect wirelessly to the pacemaker once a day, collect log information from the pacemaker, and send

that information over the internet or over the telephone line to the vendor's server, and then there is a web interface that the healthcare providers can log into to retrieve your patient information.

Can hackers break my heart? To answer this question, I decided to use the competence I have on IT security, unlike most patients that get the pacemaker at an older age. I started a project together with some of my security research friends, we were trying to figure out if and how it can be hacked. How is the data generated by my own body, my own heart, secured? Is it possible for someone with malicious intent to obtain access to my implanted device remotely via the communication interfaces? These are some of the questions I tried to figure out in my research project, because with connectivity comes vulnerability, and as a security researcher I am worried, because I know that our society is adopting connected technology faster than we are able to secure it.

Part of the problem with doing security research in this field is that the code in my pacemaker is not available for me or other security researchers to look at. As a patient, I am expected to simply trust the vendors when they claim that their devices are not vulnerable, but as a security researcher, I want to figure out by myself how things actually work, and in this case, it meant going on eBay, purchasing used medical equipment and hacking it.

We are looking at several models of pacemakers in our project. Several of these have been donated to me by supporters of my project, which I am really grateful for. I am, of course, not running tests on my own implanted pacemaker in this project. In one of our experiments, our researchers captured the communication signals that are transmitted from the pacemaker. But to find out how secure pacemakers are, we open them up, and we try to find out how they are constructed and how they communicate. This type of hacking is called reverse engineering, meaning that we have a finished product, and we try to get into the minds of the engineers that build it, searching for vulnerabilities in their implementation. We examine to see if they make any mistakes when designing building or coding the software inside of the pacemaker inside of my body. I sometimes picture the person programing the code that is running inside of my body, did he have a good day at the office?

Of course, this hacking needs to be done in a responsible manner. This means that the vulnerabilities that we find in this project will not be publicly released and disclosed before we have worked with the vendors to solve it and find fixes to the problems. I do not want to scare fellow pacemaker patients or make anybody avoid receiving lifesaving treatments due to fears of hacking. But it is already established by previous research that pacemakers and other medical equipment can be vulnerable to hacking. It is possible to extract sensitive and personal information from pacemakers and to threaten a patient's life by turning it off or changing its pacing behavior. Fortunately, certain attack that has already been proven to be possible requires close proximity to patients, and it cannot be carried out remotely.

Hacking of pacemakers through their internet connectivity, like you may have seen in popular TV shows, has not yet been proven to be possible; however, no independent research looking into this more closely has been published. Patient safety is not only threatened by actors with ill intentions; devices can also deliver the wrong treatment because of human errors or software bugs. I am here today to tell my story, but others do not have this opportunity. Think about that. In one case, 13 patients died because of faulty cardiac devices. In 2005, two doctors went public with concerns after a 21 years' old patient died when his implanted cardiac defibrillator short-circuited and failed to revive him when he went into sudden cardiac arrest. The vendor had known about this short-circuiting issue since 2002, and had made two attempts to fix the device, according to the court documents, but the company did not alert the medical device regulator in the USA, the FDA, so that they could issue a recall.

I have personally experienced how it feels to have my heart controlled by a machine that is not working correctly due to a software bug. Since I am younger than most pacemaker patients, the default configuration settings were not suitable for me, and it took a few months of trial and error and tweaking before the doctors could figure out how to get the tuning right. This was complicated because of a software bug in the programming device that they used to adjust the settings of the pacemaker, and the consequence of this greatly affected my well-being.

Two weeks after my surgery, four years ago, I went to London with some of my colleagues to attend a course on ethical hacking and incident response. This was the first time I realized that something

was wrong with my pacemaker. We got off the train at Covent Garden underground station, and there were long queues to the elevators, so we decided to take the stairs. They do have a warning sign there for people with heart conditions, saying that they should not use the stairs, but clearly I did not read the sign. While I was climbing the stairs, suddenly I was out of breath, I felt like I could not go on. You can compare to the feeling you get if you start running as fast as you can up a hill, and then you come to a point where you are exhausted, you can't make it anymore, expect that this happened to me in an instant, and I had no idea what hit me. I realized it must be connected to my pacemaker.

After returning from my trip, I went for a check-up to see if they can figure out what happened to me. At the hospital, the pacemaker technician examined my pacemaker, controlling my heart with a touch of a pen on the touchscreen of the pacemaker programmer. The hospital has a stack of different programmers from the different vendors, because they all communicate in different, non-standard ways with the implants. There are buttons for making my heart go faster, slower, or even for turning off the pacing completely. The problem in my case was that the number shown on the programmer screen, indicating the upper heart rate limit of my pacemaker, was not the same number as the actual settings of my pacemaker.

Because of this software bug in the pacemaker programmer, it took several months to resolve my problems, and during this time I would get into the same feeling of exhaustion whenever I was trying to run after the bus or walk up some stairs. Basically, the pacemaker was programmed to suit the activity level of an 80 years old patient, and it would malfunction whenever my pulse hit 160 beats per minute. They eventually figured this out, and despite the programmer bug, today the pacemaker works perfectly, and I even finished running a half-marathon last year with the pacemaker. I am lucky, because technology saved my life. I would probably not be here today if it wasn't for the pacemaker. The decision to implant a medical device is also a risky one, but in my case, the benefit of having the device clearly outweighs the risks.

On my spare time, I am volunteering for the grassroots organization I Am the Cavalry. We are focused on issues where computer security intersects with public safety and human life. We work to improve

visibility and awareness of these issues while preserving trust. We collaborate among all stakeholders and deal with their concerns, to try and find the common way forward, where everyone wins. Recently we published the Hippocratic oath for connected medical devices. These are five steps that we want the vendors of devices to adopt to make them more secure for the future. No patients have, as far as I know, been killed due to a hacker pacemaker, but patients have been killed due to malfunction of their medical devices, configuration errors, and software bugs.

In the future, many of you will live longer and healthier lives because of implanted medical devices and different types of sensors in your bodies, but this technology might also kill you if not implemented correctly. This is some of the research I would like to see in the next 5-10 years, because security research in the form of preemptive hacking, followed by coordinated vulnerability disclosure and vendor fixers, can help save human lives. This is why I am calling up on the technology enthusiasts among us, the hackers, the tinkers, the doers, to do more research on medical devices and implants, and join me in hacking to save lives.

PROF. MORAN CERF, PROFESSOR OF NEUROSCIENCE, KELLOGG SCHOOL OF MANAGEMENT, NORTHWESTERN UNIVERSITY

I will tell you a few things about how neuroscience, and how my field of research informs cyber security, and tries to use what we know about the brain to challenge our abilities to think and to reflect on security in the years to come. I will also try to reflect on what happened to me and to the field over the past four years. Over those years, the things we dealt with have gone deeper and deeper into an understanding of the brain and what it can tell us about neuroscience.

In 2012 I spoke about hacking the human body, and today insulin pumps or defibrillators and pacemakers can actually allow us to do something that changes people's behaviors. At the time it seemed like a futuristic thing, but now, with the ability to edit genes in a living human, we know that there are ways to change your traits and personality even after you are born, just by doing things that affect your body.

In 2013 I spoke about how to use neuroscience to extract information from the brain, the idea being that we have a greater and deeper

understanding of how brain functions work, and what controls which cognitive aspects, and we are now intently looking at the science that has to do with familiarity. We can show you passwords, and know whether or not you recognize a layer, a character or a digit in them. We can look at parts of the brain that come to life when you look at your password and see if your password has a semantic meaning, if it is a word that you recognize or a scrambled set of characters, and we can start learning something about your choice of passwords just by looking at the brain. The reality is that the only thing that stops us from being able to read entire things in the brain is just the resolution of acquisition devices – the better we become in looking at the individual neurons in your brain and seeing how they work, the more likely we are to understand more and more about your passwords.

In 2014 I spoke of a project by a colleague of mine at Stanford, Dan Bone, who researches ways to place passwords in your brain, without you knowing what they are. You can use them when you are confronted with a problem, you can actually express the password when you type it, but you have no idea what that password is. It is sitting in your brain, and it relies on the fact that we can train you to do things and stick information in your muscle memory without having you actually know the information; no matter how much torture you would undergo, you would be able to actually give me the password only when I ask you to type it. Although this is mostly a theoretical idea, right now we are performing a series of experiments showing that people can learn, after 30 minutes of playing a game, something about the code of the game, and then two days later, when they are asked to play the same game, we can tell who was the person who was trained before and who wasn't.

In 2016, there are three fields where neuroscience is making progress, trying to understand how we can use understanding of the brain to also inform security. These are the fields where we try to understand how we can make people do things regardless of whether they want to do it or not. How we can make people see different things than what their senses offer, or how to make them think things that weren't there before. Essentially, in the aspect of hacking, we are trying to see how we can hack our sleep, hack our perception, and hack our cognition. I will give examples of those three fields, from experiments that are currently being run, which allow us to imagine a world where

those three things are going to be something that hackers could use to challenge our perceptions.

Hacking our sleep: over the past year I have been involved in several studies that try to go into the fortress of the human mind, and actually change how it works. Think about your brain as a little fortress that encapsulates all of your information, all the things you learned, your memories, your feelings, your decision-making processes. Your entire character sits in there, however, unlike any bank or financial institute that you really protect well, with firewalls and VPNs and application securities, this fortress actually removes all of its guards for a third of the time when you are asleep.

Every day, for about a third of the time, we go to sleep and essentially have our brain go into Safe Mode, where it doesn't really protect itself anymore. It is as if you have a company that for eight months of the year uses the most complex security, but for four months has no security measures. This is how our brain works. We have a period in a day where our brain doesn't really protect itself. This is a curious evolutionary question, why do humans have such a brain? If we look at other animals' evolutionary trees, we can see that many animals solved their problems in this aspect: dolphins go to sleep one hemisphere at a time, so that they have half of their brain awake even when they sleep, in order to protect themselves; birds can even fly while they are sleeping, because the part of the brain related with muscle control is still awake even while they are asleep. But only us humans are turning off for four to eight hours a day and are basically essentially entirely vulnerable.

Sleep is an even more curious process, because it turns out that when we let our guards down, our brain still keeps working, it just does things that are not entirely under our control. Specifically, what we know now is that sleep is broken into stages, and that some of those stages – notably one known as the slower sleep process – is a time where your brain evaluates the day and decides what to make of it. It can be compared to a database of all your memories and experiences of the day sitting on one side, and overnight, in a specific moment, your brain selects some of those moments that it deems important, and moves them into long term memory, a better and safer storage environment, where it is going to be used in the future to make better decisions.

You can't store everything, so overnight your brain chooses some the more important memories and moves them, and the rest is suppressed or entirely erased. The way the brain chooses that is by a very complex process that relies on years of evolution. As of the last two years, we are starting to understand how this process works and when it happens, to the point where we can actually do things to the process that change the way it works.

There is a famous study in rats and mice, where they were given beta blockers, particular pharmaceuticals that stop the process from happening, essentially rendering the memory inactive. In this scenario, the memories of the rat are not transferred from one side to another during the night, but are lost instead, because nothing actually stores them in the right place. We can't do that in humans yet, but we can shape the process. It turns out that in a very simple way, using smells and tastes and touch, and things that actually penetrate your sleep without waking you up, we can trigger your brain into choosing some memories but not others that we select for you. If I give you the right smell, I might change your pointers so that you will choose one memory over another, and store that rather than this. Essentially, I can choose for you which information will be going from your short term memory into the long term memory.

When you go into this dimension, you can imagine a world of opportunity; we can actually measure and maybe change your preferences overnight into choosing one versus the other. For example, when you wake up in the morning, I would ask you to renew your password for websites, you would randomly and intuitively and by yourself choose a password, only that we learn afterwards that overnight I selected for you the things that are going to be in your cache memory, and the password that you chose is going to be triggered by me overnight, where I nudged your brain into one direction rather than another. This is not science fiction, we are already doing something like that in the lab; we have participants that go to sleep, and overnight we nudge their behavior a little bit, and when they wake up they have to make a choice, which we affected. This time we are focusing on health choices, so we make them choose salad rather than a steak, but the idea is the same – I chose for you overnight something that when you wake up in the morning, you will think you selected yourself, while actually you were under my spell.

Hacking our perception: we can imagine a process that all hackers know as "race condition", when there is one system here that gets information, another system that feeds information, and the two of them assume that they speak the same language. In our case, information from database one goes to storage two you don't authenticate anything anymore. This is how our brain works.

Our brain on the inside doesn't really authenticate each process, so this part of the brain thinks whatever came from that part of the brain is just clearly the same as it was determined to be. If I can come in-between and change information inside your head, I can essentially make your brain store information that it thinks comes from itself, but actually came from me. One of our participants uses a cochlear implant, a device that tells the brain what is out there, what the brain thinks it is hearing. When you think of the brain, you think about it as seeing, hearing, smelling, and tasting the world, but in reality, this is not the case. Our brain is sitting in a very safe place, under a structured bone, it doesn't see anything or hear anything, it doesn't even have access to the world. All it has is a bunch of liquids that surround it in a very rigid area that prevents it from moving. The brain sits in a dark place full of water, and all it knows about the world comes from plug-and-play devices that feed into it: your eyes or your nose or your ears.

There is a contract between your brain and those devices, saying that whatever comes from them is real, but this contract is only true because no one challenged that. If you look at the world right now, what you think you see is the entire world, but we know it isn't the case, because, for example, our phones emit rays of cellular reception, and even though we know they exist, we can't see them. A bat would be able to see these rays and fly between them, because its plug-and-play devices are aware of the rays that come out of your pockets. The bat can see the rays because it has an echo-locating device that is sensitive to them.

The brain of a bat and that of a human are very similar, with almost the same senses and functions at the neuron level. If I could take the bat's eyes and connect them into a human brain, that brain will get signals and will learn how to process them, and start seeing more of the world. We know that what we see with our eyes is only one trillionth of what is out there, and that our brain is able to see much more, but our eyes don't have the capacity to do it; and because the brain can do

those things, we can actually feed a device like the cochlear implant into our brain, have this device learn how to pass molecular changes in the air, and have the brain learn over time how to hear, even if it didn't hear anything before. The same idea works for all animals. You can take any animal with low eyesight, and add devices that allow it to touch the world.

The idea is that we can actually tell our brain that what it gets isn't reality, and feed more information into it and allow it to pass more information. But if we go into this domain, we can also imagine someone using it against us. I can actually feed into your brain more information, making you not see things that are out there or see things that are there. We can take subjects in experiments and put goggles on their eyes that take the ray of light that their eyes don't recognize but have a sensor that they recognize, feed those into their brain, and have them wear goggles that show them more of the world, such as the rays of cellular reception. Those are translated into something that the eyes can see, and after a week of wearing those goggles the brains of those people actually start seeing the rays, and start walking in the room avoiding cellular reception sites. This means that within one week the brain can learn to see more things if you just give it a new plug-and-play device, and if you go into this domain, we can understand how the brain, which has one side that just sees and another side that senses, can allow itself and ready itself for a person to come in between and change our perception, to hack what we think of as reality.

In the third and last experiment we try to hack cognition. We think that cognition is what makes us human, but we know from games like Jeopardy, that was played in a "human versus computer" version five years ago, that actually the field of AI and machinery allows us to mimic the way the brain thinks, and create machines that essentially behave like us. Machine learning algorithms don't really know the answer to a problem, they just get many examples, and somehow find the rules that govern those by themselves, somehow mimicking the way we think. We don't really teach people things by telling them "this is the rule of how language works", we just show you many words, play many sounds, and have you somehow, as a child, learn a language, or learn how to move, or learn how the world works. This means that more and more algorithms are controlling the world around us and making choices for us.

Notably, one of the biggest hacks in the world, the biggest theft of money to date, happened on May 6th, 2010, and it was a theft at the amount of $1.2T. It was done by an algorithm known as the "Flash Crash of 14:45". On May 6th, 2010, at 14:45, the New York stock exchange suddenly experienced a huge theft of money. Stocks at the amount of $1.2T, which is almost the USA's debt to China, disappeared randomly, and fortunately came back after 20 minutes. To this date, no one knows what faulty algorithm led to this loss of money, and fortunately the same algorithm decided to bring the money back, but if it hadn't done that, we would still be chasing the largest sum of money stolen without having a person to blame, because it all happened by a computer.

In the same way, algorithms are now governing our preferences. The most expensive book on amazon to date is this book called "Making of a Fly", a textbook in entomology, insects and their lives. It has about 100 copies sold a year, even though it is out of print, and these are mostly used books. Its price in amazon right now is $1.7M, even though it doesn't exist, and no one prints it anymore because it's sold in the used book market. If you buy this book right now for $1.7M, you would actually make a bargain, because when it was up for sale people started noticing that the price went up to $23M, plus $2.99 shipping and handling costs. Why is that? Because this book is sold by an algorithm that decides by itself what is the interest right now, and raises or lowers the prices based on what people think. We now outsource choices of sales to algorithms that try to think like we think, and try to make profits like we would, only they have no sense of insights about what makes sense, to the point that they make such mistakes. More and more, we have algorithms deciding for us what we would like if we bought a certain book, and which other books would be relevant. We have TV shows that use that fixed algorithms to decide how to cast characters in the show based on your preferences, and we even have algorithms that are smart enough to know what is embarrassment, as in they offer us movies that we would enjoy watching but will be embarrassed having our friends know that we enjoy watching.

Those are algorithms that know something about us that is very human, and we can't articulate perfectly but they can. Those algorithms even have a sense of what "clean" is. They have different ways to clean our room, thinking that they know something about what we prefer, and

ultimately, as we become dumber, they become smarter. In 2016, more people are going to die from extreme selfies than from shark and crocodile attacks. And we allocate more and more of our thinking to machines that do it for us, and it becomes interesting for me not in the place where we actually allocate our cognition to computers, but in the idea that we still think there is something that saves us. However, I don't think this is the case.

In the famous Jeopardy game played by humans against computers in 2011, the computer won. This is not surprising to you, but what is surprising is that there is one moment that was entirely overlooked, which I find to be the most telling moment. This was the moment where the computer was able, for the first time, to top the humans. Humans were leading for a while, but then the computer started answering questions and took the lead, and the human got really upset because he tried to press the button fast enough, but he was just too slow for that. And so it continued – the human was too slow, and Watson the machine got better and better and started leading over the human. However, at some point the human managed to press the button quickly enough, but didn't know the answer to the question, so he paused to think, to come up with the answer. Computers are faster than humans, and better at collecting information, but humans rely on a unique ability to produce insights, something that allows us to press the button before we know the answer, and wait for our brain to come up with that.

I spent the last winter working in CBC trying to help TV writers come up with a TV series about hackers and the brain, and at some point I offered them an interesting idea: what if we have an episode where the machines win and humans lose? And they laughed and said no, no one is going to want to watch a TV show like that. The reality is that right now, in Hollywood, all of our movies are made in a specific protocol where first there is a battle between the humans and the machines, we build them and they become smarter and tougher than us, and they start beating us in things; but somehow, even though it seems like we are going to lose, it comes to minute 75 in the movie, towards the end, and through the virtue of insight or love or intuition, humans take over and win. What I find scary is that Hollywood makes those movies the way they make them only for one reason: because right now the movies are made for humans. Once computers are going

to start making their own movies, we are going to have the same beginning, but come minute 75 there is going to be a battle between us and them, and because of the virtue of insight-love-emotion they are going to destroy us, because that is one thing that makes us human, which may have helped Peter Jennings, but still didn't let him win.

I see computers and machines learning how we think as something that helps us a lot and becomes useful for us, but also as one of the biggest threats right now, because we know only how it begins, but like many wars – we have no idea how it is going to end.

CONFERENCES' SPONSORSHIPS AND ASSOCIATIONS

DIAMOND SPONSORS

accenture
High performance. Delivered.

DISTINGUISHED BENEFACTOR

KETER

PLATINUM SPONSORS

Check Point
SOFTWARE TECHNOLOGIES LTD.

CYBERARK

EMC² RSA

GE Digital Israel

IAI
ISRAEL AEROSPACE INDUSTRIES

IBM

Microsoft

TEAM8

THETARAY

YL VENTURES

GOLD SPONSORS

CYBERBIT
PROTECTING A NEW DIMENSION

EDO
Technologies ltd.

FORCEPOINT
POWERED BY Raytheon

FireEye

QUALCOMM

REDDOT
CAPITAL PARTNERS

TEMASEK

Steven E. Stern

SILVER SPONSORS

IATA

SAP

Telit

In association with

comtec
Conventions & Special Events

#BIGIDEA

CDM
CYBER DEFENSE MAGAZINE

Cellcom

CII
Confederation of Indian Industry

CYBERTLV

ICEX
España Exportación e Inversiones

IEEE

אוניברסיטת תל-אביב

IATI
Israel Advanced Technology Industries

ISRAEL-BRITAIN CHAMBER OF COMMERCE

ITA
ITALIAN TRADE AGENCY
ICE - Italian Trade Commission
Trade Promotion Office of the Italian Embassy

MARKET RESEARCH MEDIA
your unfair competitive advantage

Ministry of Foreign Affairs
Israel

NOVAWIND
BOOSTING BUSINESS

OurCrowd

SAGIV TECH

STARTAL

UK Israel Tech

הארץ
TheMarker

גבהים

מגעים

רכס
פרויקטים חיוניים בע"מ

TEL AVIV UNIVERSITY
ALUMNI ORGANIZATION

תל אביב יפו
TEL AVIV YAFO

Interdisciplinary academic research has a crucial role to play in cybersecurity. The first 2011 Annual Cyber Security International Conference at Tel Aviv University has attracted top political, industry and academia leaders and experts from Israel and the world, on stage and in the audience. The following annual events saw the line-up extended, dedicated tracks added, and enjoyed attendance of over 5,000 participants each.
The Proceedings of the fourth and fifth Annual Yuval Ne'eman Workshop for Science, Technology and Security Cyber Security Conferences publication will enhance the global impact of the work presented at Tel Aviv University.

The Yuval Ne'eman Workshop for Science, Technology and Security was launched in 2002 by Prof. Isaac Ben-Israel in conjunction with the Harold Hartog School of Policy and Government and the Security Studies Program at Tel Aviv University, to explore the nexus of science, technology and security, and to addresses policy-relevant issues with rigorous scientific research. The Workshop engages topics of international relations, strategy, cyberspace and cyber security, space policy and space security, precision weapons, robotics, nuclear energy, homeland security, and the interplay between society and security. The Workshop organizes a range of conferences, panels and expert meetings, and maintains working relationships throughout the academia, business, policy and defence circles.

The Blavatnik Interdisciplinary Cyber Research Center (ICRC) was established at the Tel Aviv University as a joint initiative with the National Cyber Bureau, Prime Minister's Office.
The Center is based on researchers from Tel-Aviv university and emphasizes the importance of interdisciplinary research. Currently, there are 50 faculty members and over 200 cyber researchers from different faculties such as Exact Sciences, Computer Sciences, Law, Engineering, Social Sciences, Management and Humanities.
The Center aims to become a leading international body in its field and to increase the academic efforts and awareness in the field of cyber security.
Research topics at the Center include key issues such as security software, attacks on hardware and software, cryptography, network protocols, security of operating systems, and networks as well as interdisciplinary research such as the impact on national security, the impact on society, regulation, and the effects on the business sector.
The Center operates a research fund which is supported by the National Cyber Bureau.