SDA
SECURITY & DEFENCE AGENDA

Microsoft

SDA Report

Cybersecurity: Is technology moving faster than policy?

A ***Security & Defence Agenda*** Report
Rapporteur: **David Koczij**
Photos: **Philippe Molitor**
Date of publication: **February 2011**

SECURITY & DEFENCE AGENDA
Bibliothèque Solvay, Parc Léopold,
137 rue Belliard, B-1040, Brussels, Belgium

CONTENTS

At a glance—Speakers and moderator 2

Introduction 3

What challenges need to be overcome for a secure cyberspace? 3

Some issues and accomplishments for the European Union 5

Future developments for improved cybersecurity 7

Conclusion 8

List of participants 9

About Microsoft 11

About the SDA 12

Cybersecurity: Is technology moving faster than policy?

Policymakers' dinner
Monday 31 January 2011
Sofitel Brussels Europe

Cyberattacks in Europe and across the globe are at an all-time high and showing no signs of abating. Remote hijacking of computers for malicious purposes constitute an "electronic epidemic". Faced with such rapid technological upheaval, European policymakers seem slow to react. As EU member states rush to create the necessary national agencies, is it time for a European cybersecurity authority? What technical capabilities would such a body need, and who should provide them? Under which jurisdiction should cybercriminals be prosecuted? Is a stronger private-public cooperation framework needed to support such a system? Can the need to provide a safe cyber environment be balanced with privacy for the individual? Could investment in public education for "good hygiene" practices offer a low cost answer to the threat of viral infection?

Speakers

Mario Campolargo
Director, Emerging Technologies and Infrastructures
European Commission
Directorate General
for Information Society & Media

Craig Mundie
Chief Research and Strategy Officer
Microsoft

Jamie Shea
Deputy Assistant Secretary General
NATO Emerging Security
Challenges Division

Moderator

Giles Merritt
Director
Security & Defence Agenda

Policymakers' dinners offer specialists in a defined policy area an opportunity to discuss issues with key officials of EU, NATO and diplomatic representations, and leading figures from NGOs, business and industry. The dinner format lends itself to free-flowing debate and an open exchange of views.

Cybersecurity: Is technology moving faster than policy?

Introduction

With the continuing increase in the number, scope and severity of cyberattacks around the globe, it seems that the EU, NATO and their partners are lagging behind in crafting effective policies to meet the demands required by ever-evolving threats emerging from cyberspace. The participants at the Security and Defence Agenda policy-makers' dinner on 31 January 2011, entitled "Cybersecurity: Is technology moving faster than policy?", agreed on the need for a common typology of cyberthreats and security policy responses, to be drafted in collaboration with public and private actors.

Over the past decade, began **Craig Mundie**, Chief Research and Strategy Officer at Microsoft, there has been a shift towards ever-increasing connectivity of networks around the globe. As the software technology on which these systems run evolved in a secure and benign operating environment, the systems have lagged behind from a security perspective.

"This remarkable internet connectivity," he explained, "which has brought so many benefits, has also brought a set of risks from those who choose to use these tools to exploit system weaknesses. While we who develop these technologies are greatly improving the way we operate, the community of 'bad guys' has become very efficient as well."

"There is a growing awareness that cyberthreats can be detrimental to business, competitiveness and economic growth," offered **Mario Campolargo**, Director for Emerging Technologies and Infrastructures at the European Commission's Directorate General of Information Society and Media. While the European Union provides a lot of funding to the research and development of new information and communication technologies (ICT) in order to address existing and emerging problems, "security cannot rely solely on technology. In fact, policy must, and will, play a crucial part in this area." Referring to the Digital Agenda for Europe launched by Commissioner Neelie Kroes last year, he added that "developing trust and security in the online environment is a priority for the EU's digital agenda."

"Cyberspace is another episode of the human saga of coming to terms with anarchic space, in the same historical vein as sea, air and space."

"Cyberspace is another episode of the human saga of coming to terms with anarchic space, in the same historical vein as sea, air and space," offered **Jamie Shea**, Deputy Assistant Secretary General, NATO Emerging Security Challenges Division. Important details aside, he continued, "the basic point is that we are all together in this world for the duration. What the EU, NATO and their partner organisations need is an intellectual revolution and to find the strength to make the decision to relegate more intellectual resources to questions of cybersecurity."

What challenges need to be overcome for a secure cyberspace?

As technology permeates society, security and trust in information and communication systems becomes a significant factor in their development, participants heard.

Following his work on Microsoft's Trustworthy Computing Initiative, Mundie noted that there are four elements to maintaining users' trust in computing systems: security, privacy, reliability, and interoperability. Although the high-technology industry has worked diligently over the past decade to create trustworthy systems based on these four criteria, the challenges in these areas remain, he concluded.

The most potent emerging challenge in cybersecurity has to do with the changing uses and capabilities of cybertechnology, Mundie explained. "Intelligence and defence services of many countries now realise that these technologies are critical to their mission on the intelligence-gathering side as well as a serious threat on the operations side." It is the responsibility of national and international agencies to engage themselves with the technology and policy surrounding cyber in order to tackle the duality of the issue.

Speaking from a military strategist's perspective, Shea asked the participants to consider the fact that, while in the past cyber was used primarily for espionage and intelligence gathering, it has increasingly been used for denial of access and even destructive attacks. "We must consider how much cyber changes our thinking about conflicts," he stated. "Will states now resort to the softer power of cyber interventions where before military action was the norm?"

"No matter where things like the Stuxnet program emanated from, it should be a wake-up call that strictly software-based attacks on systems can now wreak real and substantial physical damage," agreed Mundie.

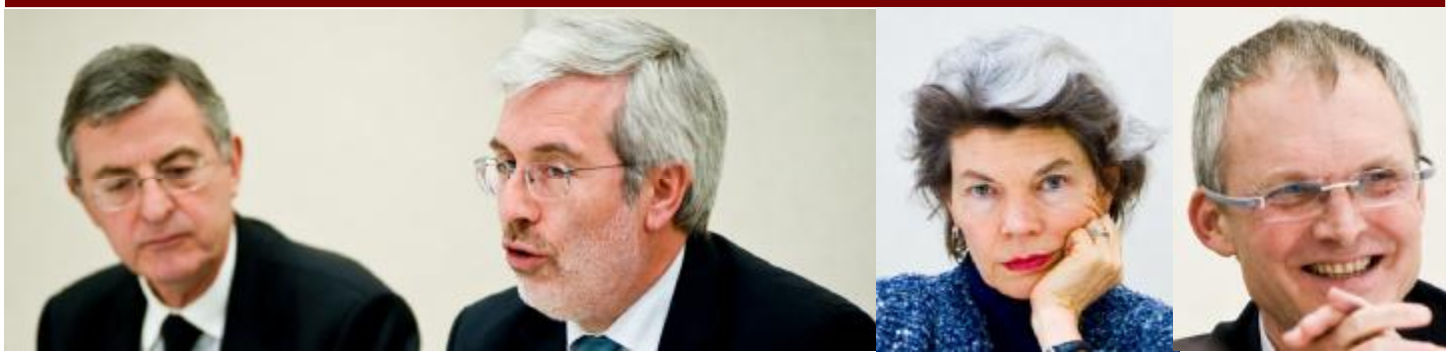
"No matter where things like the Stuxnet program emanated from, it should be a wake-up call that strictly software-based attacks on systems can now wreak real and substantial physical damage."

The problems emanating from cyberspace go beyond state actions, Shea continued, stating that "cyber has allowed the private individual, organised crime, terrorist groups, social misfits and hacktivists to get involved with areas that were previously state-controlled."

In fact, said Mundie, cyberattacks have evolved from 'malicious mischief' committed by certain individuals seeking notoriety to attacks of a criminal nature – people seeking economic and ideological gains rather then notoriety. This has had the effect of reducing the visibility of such attacks while escalating the seriousness of their consequences.

The increasing severity of cyberthreats is closely linked to the increase in connectivity that the world is witnessing through, for example, cloud computing, continued Mundie. As it currently stands, mission-critical systems can by and large continue to function if temporarily severed from the network. If, however, the current trends of connectivity and interoperability continue – connecting large-scale enterprises to super-scale activities – government and industry will have to carefully weigh potential efficiencies and economic returns against the fact that consolidated system architecture is exponentially more vulnerable to cyberattacks than stand-alone or small, protected systems.

"I think that the challenges, even as we seek to get a handle on them in the traditional environment, are going to accelerate quite dramatically, largely because the sys-



tems comprising the mobile internet are in some ways where we were a decade ago in terms of their security architectures and because of how they are developed," Mundie said.

It is projected that in 2012, more smartphones will be sold than personal computers, Mundie added, explaining that "communications technology is branching out into new areas of connectivity that we, as government and industry, have not even thought about. It is going to take a really diligent effort by the entire industry to take the security technologies employed in the traditional computing space and adapt it to smartphones." Failing in this regard will make it more possible for asymmetric threat actors to attack larger and larger areas of connectivity.

Above and beyond the technical challenges facing security organisations and policymakers is the question of a common taxonomy for the different modalities of cyberattacks, the participants agreed. There has been an evolution in the terms used to describe cyberattacks, Mundie explained. The question of what constitutes 'cyberwar', 'cyberterrorism', 'cyberattacks', and so forth, needs to be agreed upon by governments, industry and international organisations before being codified into law.

"There are few laws that make cyberattacks a crime," agreed Shea. "We badly need common definitions that can be agreed upon by all." He cited the example of the 'Love Bug' virus, released by two individuals from the Philippines in 2000, which wreaked havoc on systems worldwide. The perpetrators of the attack were released shortly after their arrest because their crime was not actually against any laws in their home country.
A final challenge facing the EU, NATO and their partners comes from within their own security and organisational structures, Shea concluded. As attack capabilities move exponentially faster than defence – especially in the increase of viruses – some of the greatest lapses in security are due to poor system configurations, faulty passwords, inadequate training and lax personnel.

> *"There are few laws that make cyberattacks a crime."*

NATO is still two years away from cyberdefence systems being under one umbrella, he told the participants. "Only twenty five percent of cybertheft is deliberate hacking," he offered, "you would be surprised at how many times it occurs as a result of someone forgetting a USB stick on a train. You cannot guarantee that you will not be burgled but, if you lock the door, it will be harder to get in."

Some issues and accomplishments for the European Union

The Digital Agenda for Europe has had some success in creating and aligning European policy on cyber, began Campolargo. One of the milestones he referred to was the Commission's communication on critical information infrastructure protection (CIIP), approved in March 2009. The CIIP strategy is based on 5 pillars, he explained:

- preparedness and prevention;
- detection and response;
- mitigation and recovery;
- definition of criteria for the identification of European critical information infrastructures; and,
- very well developed international cooperation.

All of these pillars are described in the Digital Agenda, as

well as a set of concrete actions that have been taken to achieve them. These include the development of the European Public-Private Partnership (PPP) on Resilience, a project aimed at working through a forum of EU member states and industry on issues such as resilience and defining baseline capabilities for national governments. Another successful area of action has been the creation of a Computer Emergency Response Team (CERT) for the EU institutions, focussing on national contingency planning and exercises, as well as pan-European exercises on large-scale network security incidents.

"Ensuring necessary levels of citizen security and trust in the digital society in order to realise its full potential and to promote eCommerce, eGovernment and eHealth while at the same time safeguarding fundamental values such as privacy and personal data protection."

However, Campolargo continued, cybersecurity is not only about protecting state secrets and vital services, nor combating cybercrime. It should also be about "ensuring necessary levels of citizen security and trust in the digital society in order to realise its full potential and to promote eCommerce, eGovernment and eHealth while at the same time safeguarding fundamental values such as privacy and personal data protection." In this context, the revised European ePrivacy directive aims to protect the end user from the risks of cyberattacks, he concluded.

In addition to the policy side, added Mundie, there are new technological approaches to dealing with privacy issues. "Privacy concerns stem from the capacity to aggregate and scan data. Up until now, however, no one has asked our industry's software engineers to develop a protection mechanism against these capacities." Though optimistic about the technological solutions, he did admit that a lot of the data privacy debate in Europe has to do with unaligned regulations and norms between member states.

With so many divergent cultural backgrounds in the EU, it is difficult to harmonise and regulate single rules, agreed Campolargo. "Though harmonisation is a long process, we have taken some strong first steps towards achieving common rules, including a European Forum for member states and the involvement of the private sector though PPPs."

As global systems continue to witness exponential growth in traffic and connectivity, the EU needs to promote constant research and innovation in the area of ICT, participants heard. In its policy proposals and funding regimes, the Commission is privileging user-centricity, data and privacy protection and security, explained Campolargo. The ICT focus section of the Security Research Programme promoted by the Commission is working to address the challenges of network security, cloud computing, trustworthy identity management and the growing interdependence of ICT and critical infrastructure.

While addressing concerns related to technology, he concluded, it is essential to include industry. "In the newly launched PPP on the Future Internet, we will tackle the development of new public infrastructures which, as the future of our European society, must be resilient and dependable. However," he added, "the effects of pro-

grammes such as this cannot be limited to technology but must consider legal, cultural, educational, social and economic aspects."

Future developments for improved cybersecurity

The evolution of cybersecurity models was described by Mundie using a medieval analogy. "As far as cybersecurity is concerned, we began by putting up big walls. Our antagonists responded with weapons capable of breaching these walls, so we built bigger walls, and so on. We need to move away from this mode of functioning, from a passive defence model approach to an active one." In other words, he continued, it is not enough to detect and deter cyberattacks anymore. Instead, government and industry need to work together to weed out weaknesses and then strengthen the security architecture.

An important element of this process will be the acceptance of the scale and speed at which cyberattacks can occur. "We are approaching a time when the response to cyberattacks will have to be carried out without human intervention," he explained. "People just cannot respond fast enough, so we will have to put in place policy that is robust enough to allow action by security programs." To illustrate this point, he offered the evolution of the length of time required to attack across the Atlantic ocean, going from months by boat, to 30 minutes with ICBMs, to 30 milliseconds with ICT.

Developing an active defence model for cyber will require a lot of coordination between governments and industry in the context of international organisations, participants agreed. "The EU and the United States (US) have a vital interest in joint soft-power at a point when cyber is not yet out of control," offered moderator **Giles Merritt**, Director of the SDA.

Companies like Microsoft have the ability to see machines that are failing on a global level, added Mundie, explaining that, by following malfunction reports from tens of millions of computers a day, it is possible to locate cyberattacks regionally, in the manner of a seismograph. The capacity exists, he concluded, but Microsoft and other industry actors do not have the authority to act on the spread of detectable attacks owing to state sovereignty and the lack of harmonised global regulation. He called for governments to intervene in this issue and work towards developing flexible and effective global policies.

"We know that we cannot have an arms control treaty on cyber or a system of international governance tomorrow," admitted Shea, "but we can at least start having conventions agreed on in international organisations whereby a country under attack can insist that other countries cooperate by shutting down ISPs or offering help with investigations." Through this modest beginning, he added, the daunting task of creating and ratifying an overarching international agreement can be broken down into a regional process to slowly integrate a unified vision for regulating cyber.

Some participants agreed that there could be a merit to developing multiple levels of defence as opposed to a centrally focussed organisation. In the case of an all out attack, Shea stated, the paradox of cyber is that there needs to be a central authority to coordinate the system. This central system would itself be the greatest weakness if attacked directly. "In this sense," Shea offered,

"business continuity planning needs to be translated to the world of cyberdefence."

In order to ensure a more secure future in cyberspace, the cyberdefence community must also introduce a more robust identity system, suggested Mundie. "The internet was built by a bunch of friendly people who never envisioned the current problems, so we must develop a way to retrofit identity into the system." Once the anonymity of attackers is threatened, it will become much simpler to attribute attacks and follow through with preventative and retaliatory measures.

Finally, Mundie suggested the creation of a new international institution, the equivalent of the World Health Organisation (WHO) for the internet. Using the example of successful containment of the SARS virus through quarantining and intervention by the WHO, he explained that an organisation must be created that would be able to restrict access through digital quarantine to computers displaying signs of infection.

"This idea is not new," he noted; "in almost every country in the world we require people to have licences and insurance before they can drive a car, thereby reducing the threat to society. Computers that represent a threat to society must be dealt with in a similar way."

Conclusion

Merritt, referring to the title of the debate, observed that it seems that, while technology is moving faster than policy, even faster than both is the growing consensus that cyberdefence is a major problem and must be moved to the top of the agenda. Furthermore, beyond technological issues, the question of cybersecurity has a difficult cultural dimension, as can be witnessed in the recent shutdown of the internet by the Egyptian government or the high levels of censorship applied to the internet in China. "At the bottom of all this discussion," he concluded, "there is a geopolitical divide which must be addressed."

"This idea is not new in almost every country in the world we require people to have licences and insurance before they can drive a car, thereby reducing the threat to society. Computers that represent a threat to society must be dealt with in a similar way."

"What we face is the challenge of finding the right balance between controls for the public good on the one hand, and ensuring freedom and preserving individual rights on the other," concluded Campolargo. "The pace of the digital world makes it essential to have a constant reassessment of the threat while taking account of the social, legal and economic vulnerabilities. Together, we need to face the challenges of the future digital society."

List of participants

H.E. Mrs. Pascale Andréani
Ambassador
Delegation of France to NATO

Frank Asbeck
Principal Councellor for Security and Space Policy
European External Action Service (EEAS)

Martin Borrett
Director
IBM Institute for Advanced Security

Geert Cami
Co-Founder & Director
Security & Defence Agenda (SDA)

Mario Campolargo
Director, Emerging Technologies and Infrastructures
European Commission
DG for Information Society & Media

Miguel De Bruycker
Head of Information Security and Cyber Defence
Ministry of Defence, Belgium

Ana Maria Gomes
Member
European Parliament
Subcommittee on Security and Defence

Edward Hanlon
President
Raytheon International, Europe

Scott A. Harris
President, Continental Europe
Lockheed Martin Global, Inc.

Rod Hunter
Vice President, Governmental Programs, Europe
IBM Corporation

HE. Mr. István Kovács
Ambassador
Delegation of Hungary to NATO

Cornelia Kutterer
Senior Policy Manager
Microsoft

Krzysztof Lisek
Vice-Chairman
European Parliament
Subcommittee on Security and Defence

Pauline Massart
Senior Manager
Security & Defence Agenda (SDA)

Michael Matthiessen
Director, Parliamentary Affairs (CFSP)
European External Action Service (EEAS)

Giles Merritt
Director
Security & Defence Agenda (SDA)

Craig J. Mundie
Chief Research and Strategy Officer
Microsoft

David Prichard
Chief of Staff of the CTO
Microsoft

Luigi Rebuffi
Chief Executive Officer
European Organisation for Security (EOS)

Pierre Reuland
Special Representative of Interpol to the EU
International Criminal Police Organization (INTERPOL)

Margaret Megan Richards
Director, General Affairs
European Commission
DG for Information Society & Media

Jamie Shea
Deputy Assistant Secretary General
NATO - Emerging Security Challenges Division

Thierry van der Pyl
Director, Components and Systems
European Commission
DG for Information Society & Media

Geoffrey Van Orden
Member
European Parliament
Subcommittee on Security and Defence

Henrik Vassallo
Vice President & Head of EU Affairs
SAAB

John Vassallo
Vice President EU Affairs & Associate General Counsel
Microsoft

Ronald Zink
Chief IP Counsel
Microsoft EMEA

Microsoft operates in all EU Member States, as well as in a number of other European countries. Our Search Technology Centers are located in London, Munich and Paris. Microsoft employs around 1,800 R&D staff across Europe and in 2009, we invested over € 447m in R&D.

Microsoft's 'ecosystem' of European partners includes 146,726 small and medium enterprises which generates € 120bn from solutions and services based on the Microsoft software platform.

A long-term, collaborative effort to create and deliver secure, private, and reliable computing experiences for everyone is at the heart of our approach to the evolving digital landscape.

For more information, visit please
http://www.microsoft.com/security/default.aspx and www.microsoft.eu

SDA
SECURITY & DEFENCE AGENDA

The Security & Defence Agenda is Brussels' only specialist defence and security think-tank. It brings together top-level representatives from NATO, the European institutions, national governments and parliaments, NGOs, industry, academia and the media in debates, conferences and discussion papers.

SDA Co-Presidents

Jaap de Hoop Scheffer
former Secretary General of NATO

Javier Solana
former EU High High Representative for Common Foreign and Security Policy

SAFEGUARDING EUROPE

THE SDA ATTRACTS TOP INTERNATIONAL SECURITY EXPERTS

Last year the SDA held 16 events, debates and meetings, at which over 280 senior defence and security leaders took the floor. A ground-breaking innovation was the SDA's Security Jam, which gathered 4,000 security & defence specialists from 124 countries for a five-day online discussion. In 2011 the SDA will cover topics ranging from the, reform of NATO and relations with Russia to cybersecurity and energy security—speakers this spring will include General Abrial, NATO Supreme Allied Commander Transformation, Ivan Bizjak, EU Council Director-General for Justice and Home Affairs, Peter Zangl, European Commission Director General for Humanitarian Aid & Civil Protection, Gabor Iklody, NATO Assistant Secretary General for Emergent Threats, and Craig Mundie, CTO of Microsoft.

For more information on SDA programmes and membership, visit
www.securitydefenceagenda.org

The Security & Defence Agenda (SDA) would like to thank its members and partners for their support.

The SDA gratefully acknowledges the generous support of the following governments:
Belgium | Czech Republic | Finland | France | Italy | Netherlands
Qatar | Romania | Russia | Sweden | Turkey | United States | United Kingdom

For further information on SDA membership, contact us at:
Tel: +32 (0)2 739 1582 | E-mail: info@securitydefenceagenda.org

SECURITY & DEFENCE AGENDA (SDA)

Bibliothèque Solvay, Parc Léopold, 137 rue Belliard, B-1040, Brussels, Belgium
Tel: +32 (0)2 737 91 48 Fax: +32 (0)2 736 32 16 E-mail: info@securitydefenceagenda.org
www.securitydefenceagenda.org