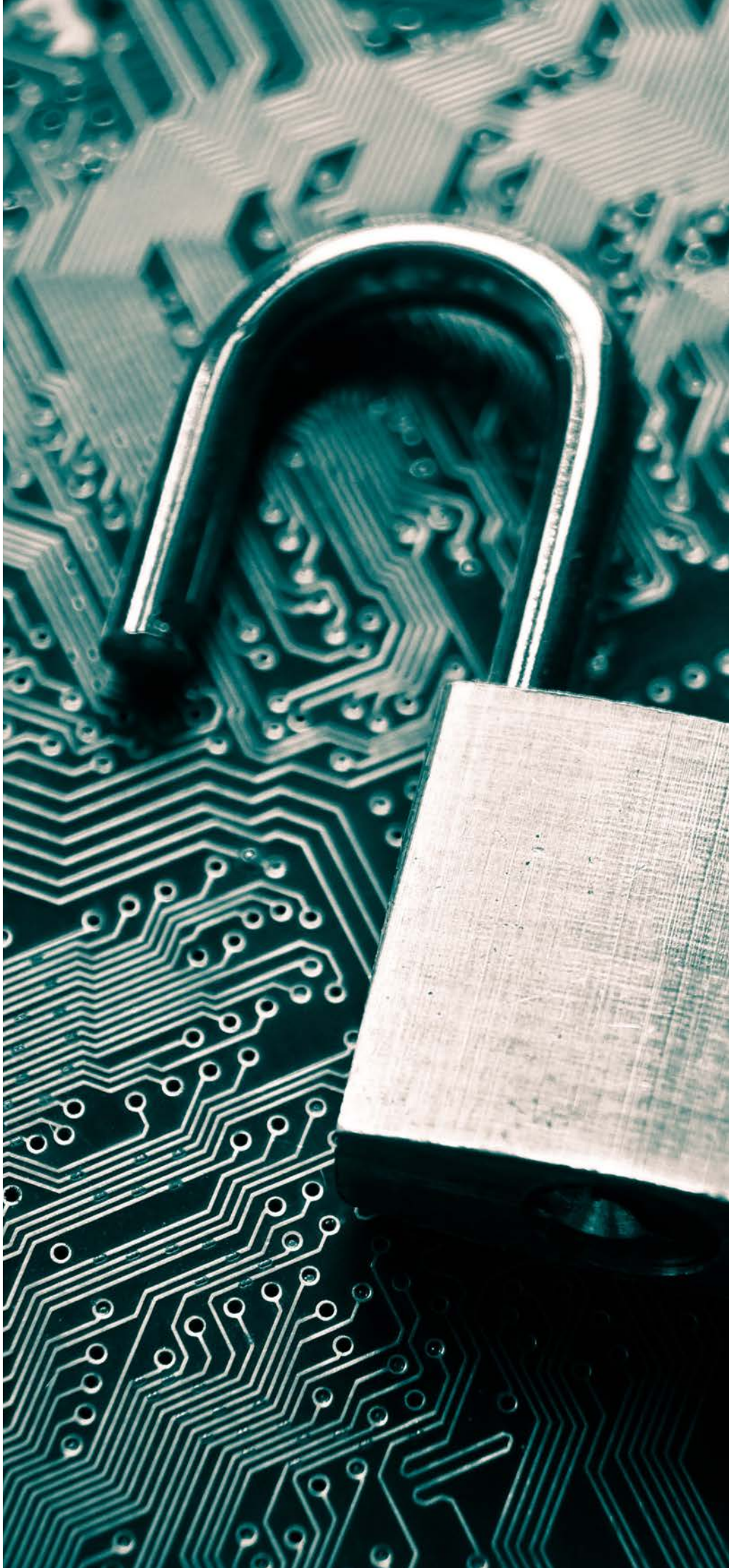
WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Recommendations for Public-Private Partnership against Cybercrime

January 2016



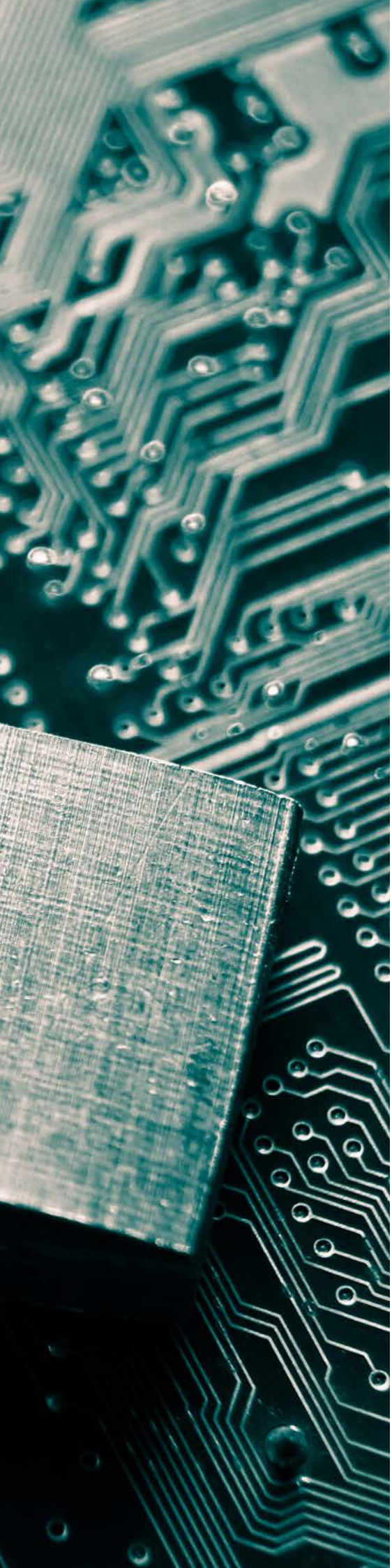
World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

World Economic Forum®

© 2016 – All rights reserved.

No part of this publication may be reproduced or
Transmitted in any form or by any means, including
Photocopying and recording, or by any information
Storage and retrieval system.

REF080116



Foreword

The world has seen much growth and development as a result of technological innovations. Undeniably, digitization has facilitated and improved the efficiency of numerous aspects of our lives, from the management of personal finance and business operations to critical infrastructure. However, along with these advances have come many disadvantages, such as the many new types of cybercrime.

The recent proliferation of cybercrime on businesses shows no signs of abating and cybersecurity is now a major concern for all business leaders – no matter what the industry, the region in which it operates and its corporate culture. All business is at risk from cybercrime and no industry wants to be targeted. If they are, they all strive to minimize the damage and recover as quickly and efficiently as possible. When speaking of cybercrime, business interests and those of law enforcement authorities are globally aligned.

Cybercrime is now an ever-present element of society. It does not discriminate between individuals, entities or governments. Everyone – and everything – is at risk. The problem is exacerbated by the ease and speed of information-sharing among cyber-criminals for perpetrating crime, making it difficult for law enforcement and businesses to keep up. Standard law-enforcement practices are not enough any longer – tailor-made tools are needed. Most importantly, law enforcement and businesses must collaborate to address this pressing issue.

By embarking on this Cybercrime Project, which is a pillar of the Forum's Future of the Internet Initiative, we have sought to gather together security, legal and industry experts – from both the public and the private sector – to help find a solution. In order to combat cybercrime in truly meaningful and effective ways, a unified approach is required. As an international organization for public-private partnership, the World Economic Forum provides a neutral platform for this range of actors to convene and deliberate and take joint action for tangible results.

The following recommendations form the foundation on which public-private cooperation for fighting cybercrime can be built. They represent the first step in a process whereby alliances can be created, giving rise to common initiatives and measures that enable better detection, prevention and more efficient combating of all forms of cybercrime on a national, regional and global level. I would like to express my gratitude to all the members of this Cybercrime Project whose dedication and participation have made the establishing of these recommendations possible. I hope they will provide the much-needed platform for future cooperation in this space.

Jean-Luc Vez
Head of Public Security Policy and Security Affairs,
Member of the Management Committee, World Economic Forum

Acknowledgements

This publication was prepared by Jean-Luc Vez, Head of Public Security Policy and Security Affairs, Member of the Management Committee, World Economic Forum, and Ushang Damachi, Project Specialist, Global Crime and Public Security, World Economic Forum

This publication was created with the input and contributions of the following individuals to whom sincere thanks and gratitude are extended:

Dominik Bark, Head Special Lines for Global Corporate in Europe, Middle East and Africa, Zurich Insurance Group

Peter Beshar, Executive Vice-President and General Counsel, Marsh & McLennan Companies (MMC)

Adam Blackwell, Ambassador in Residence, William J. Perry Center for Hemispheric Defense and Security Studies (NDU), National Defense University, USA

Jamie Brown, Director, Global Government Relations, CA Technologies

Kevin Brown, VP, BT Security, BT Group Plc

David Burg, PwC Global and US Advisory Cyber Security Leader, PwC

Alan D. Cohn, Adjunct Professor, Georgetown University Law Center

Juan Colombas, Chief Risk Officer and Member of the Executive Committee, Lloyds Banking Group Plc

Michèle Coninsx, President, Eurojust

Mark Connelly, Chief Information Security Officer, Thomson Reuters

Pär Gunnarsson, Vice-President and Chief Security Officer, Group Security, Ericsson

Jason Lancaster, Manager, Threat Intelligence, HP Security Research, Hewlett-Packard Company

John Lynch, Chief, Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice

Thomas Manson, Detective Chief Superintendent, Metropolitan Police Organised Crime Command, Metropolitan Police, United Kingdom

Marco Mille, Head of Security, Siemens AG

Christophe Nicolas, Senior Vice-President and Head, Kudelski Group

Sundeep Oberoi, Global Head Delivery – ESRM, Tata Consultancy Services Ltd

Ellen Richey, Vice Chairman, Risk and Public Policy, Visa Inc.

Jon Rigby, Director Cyber, AlixPartners

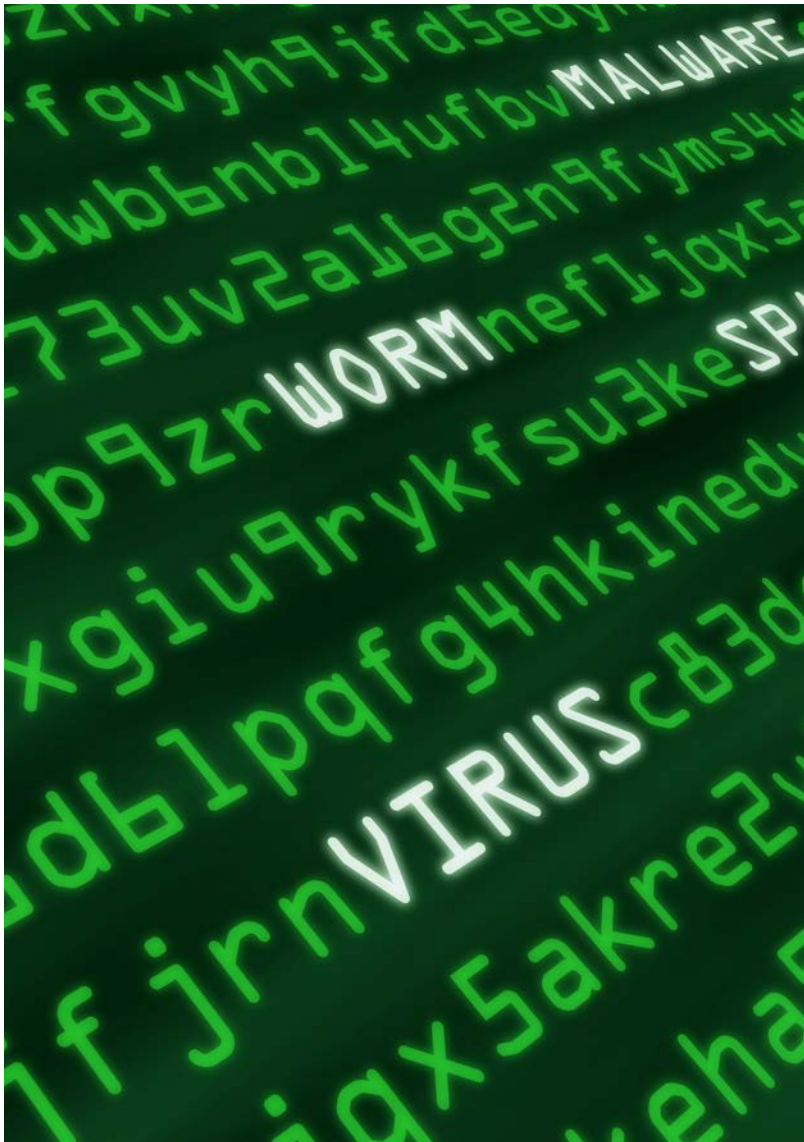
Alexander Seger, Executive Secretary Cybercrime Convention Committee, Head of Cybercrime Division, Council of Europe

Jürgen Stock, Secretary-General, INTERPOL

Bruce Swartz, Deputy Assistant Attorney-General, U.S. Department of Justice

Anne-Lise Thieblemont, Director of Global Technology Policy and Industry Relations, Qualcomm Incorporated

Rob Wainwright, Director-General, Europol



Introduction

Defining cybercrime can be a challenge as it tends to have many interpretations. For the purposes of the work undertaken by the Forum, cybercrime is a set of illicit activities that generally have two dimensions: traditional crimes that exist irrespective of the cyber world and internet but that have been, or can be, propagated and aggravated by the internet – e.g. credit card fraud, extortion, child pornography and other types of crime related to terrorism, such as preaching hatred and appeals for violence; and crimes directly related to the cyber world and internet and which cannot be executed outside the cyber sphere – e.g. hacking. This also includes items such as system interference, misuse of devices etc. as outlined in Articles 1-9 of the Budapest Convention on Cybercrime. (http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf)

What is clear is that cybercrime is of increasing global importance as it has no boundaries and targets governments, companies and individuals. Given the recent high-profile attacks on multinationals, it has become apparent that efforts must be made to find ways of tackling it. For this to be achieved, trust is essential. It is the driving factor behind productive working relationships between the public and the private sector.

Certain tools already exist in the form of laws, conventions, private-sector industry initiatives and information-sharing platforms. However, this does not suffice as cybercrime cannot be combated by acting unilaterally. Instead, the public and private sectors must combine forces to find mutually convenient ways of dealing with this phenomenon.

Through public-private partnership, the Cybercrime Project aims to evaluate existing laws and conventions, private-sector industry standards and, most importantly, encourage dialogue and cooperation on practical ways of dealing with cybercrime that are suitable to all. It is acknowledged, of course, that transparency and accountability are also essential in solving crime through public-private partnership. These recommendations, however, are the first steps in achieving mutual agreement on the fundamental actions that need to be taken to make significant global progress.

The recommendations encompass the following points:

1. Public and private sectors should share more information related to cyber threats, vulnerability and consequences
2. Public and private sectors should work to create new platforms, strengthen existing platforms, and coordinate these platforms to increase information-sharing and improve investigations and prosecutions
3. Public and private sectors should cooperate to encourage and advance wider adoption of the Budapest Convention on Cybercrime, or, of the principles it promotes.
4. Public and private sectors should work to build trust and discuss contentious topics related to cybercrime, such as encryption, cloud servers, data access and protection of privacy, to find appropriate solutions.
5. Public and private sectors can engage in other initiatives aimed at reducing cybercrime

The goal is to have public and private sector leaders support these recommendations and their subsequent implementation. These recommendations will be the first step to achieving better – and global – implementation of rules and practices enabling businesses and states (through their respective law enforcement authorities) to reduce the damaging consequences of cybercrime. The next steps will be dedicated to the analysis and practical implementation of the Recommendations.

Recommendation 1

1. **To better combat cybercrime, public and private sectors should cooperate through:**

(a) **The creation of permanent and secured information-sharing channels between law enforcement authorities and the private sector.**

(b) **The real-time sharing of information with both Computer Emergency Response Teams (CERTs) and law enforcement, related to hacking cases and to new modus operandi.**

(c) **The sharing of experiences from investigations and prosecutions.**

(d) **The sharing of technical prevention and protection measures.**

(e) **The sharing of information on technological development trends and achievements.**

(f) **The sharing of best practices related to IT education and training of end users.**

(g) **The creation of a common cybercrime taxonomy.**

(h) **The fostering of technology innovations and investment to meet global security challenges.**

Commentary

(a) Cooperation, and having the right structures in place to allow cooperation, is crucial. However, to promote information exchange and to mitigate the risk of the exchanged information falling into the wrong hands, it is essential to have secure channels in which the said exchange occurs. Sensitive information is at stake so safe methods of transmitting it between parties are necessary to ensure steady and reliable processes.

(b) Real-time information plays a pivotal role because it can avert serious disasters or minimize the effects of criminal cyber activity – it allows for quicker remedial action. Indeed, delays or data shared after the facts are not as effective. While real-time dissemination of such information might be difficult to achieve, every effort should be made to encourage the prompt sharing of information related to hacking cases and new modus operandi. This recommendation relates to the sharing of information both with government agencies and law enforcement. While the analysis of information is vital to allow for protection and patching of systems by CERTs, the role of law enforcement is equally important. It is unfavourable to share information with law enforcement only after an incident has occurred, and it has been analysed and systems patched, because it focuses on one aspect of the cyber threat – damage mitigation. Comprehensive examination of cybercrime also requires that threat-deterrent measures should also be addressed; i.e., informing law enforcement so that robust action can be put in place and criminals apprehended. Regardless of how secure systems are, cybercriminals will continue to attack them and find innovative ways of doing so unless they confronted and thwarted, hence the significance of sharing information in real-time and doing so simultaneously with CERTs and law enforcement.

(c-f) The sharing of prosecution experiences as well as technical prevention/protection measures and best practices (especially related to IT education and training) requires a commitment from both the public and private sectors to engage in this as actively as possible. Placing a greater emphasis on real-time sharing of cyber threat indicators to protect against cybercrime increases the costs for cyber criminals, and allows law enforcement authorities to focus resources on more advanced attacks. Naturally, legal constraints and requirements mean that law enforcement authorities are not at liberty to divulge all the facts and elements of an ongoing case. National legislation may prohibit certain countries from sharing any information from an active investigation with third parties. However, they can foster the spirit of collaboration – a pledge to share results of prosecutions so that reciprocal action with the private sector is maintained. Private industry often cooperates with authorities by providing a wealth of information but, due said constraints, law enforcement authorities are not a position to reciprocate. Assistance must be mutual, so ways must be found to do this.

(g) While speed and constant innovation are often cited as reasons for the difficulty in combating cybercrime, a further impediment that should not be disregarded is the varying definitions and classification of cyber-related terms. These can mean different things to different actors. Therefore, if common accord and action is to be achieved, consistency in terminology and classification must be reached first.

(h) Technology and infrastructure will need to come together in a way that is meaningful and trustworthy to users. As users and their devices will discover and interact with each other and with things through billions of simultaneous connections, they will need networks that are fast, scalable and secure. Legal and economic frameworks should therefore be adapted to treat this digital personal identity securely and to empower users to decide how their data is used and valued; in addition, high quality standards should be developed to support informed consumer decisions over their data, including its use by third parties. Such forward looking frameworks will spur innovation and create growth in a fully digitalized society.

Recommendation 2

2. Public and private sectors should work to:

(a) Create, or support the creation of, both global and regional public-private cooperation platforms to promote better cooperation between law enforcement authorities and the private sector.

(b) Encourage law enforcement authorities and the private sector to join existing public-private cooperation platforms and to enhance and increase coordination between them.

By doing so, the public and private sectors can together increase the efficiency and the impact of the fight against cybercrime.

Commentary

(a) Information-sharing platforms are essential to fighting cybercrime. It is widely accepted that combined efforts yield stronger results as various actors possess different skills, knowledge and expertise. While these may be extensive, no one actor is omniscient, hence the need for sharing knowledge. It also helps parties to learn from one another so as to better detect, protect, respond to – and recover from – cybercrime activities.

There is an abundance of information-sharing platforms across many countries and industries. However, these platforms tend to be industry- and/or region-specific. A global information-sharing platform that is based on the concept of having a truly centralized depository and exchange of knowledge can definitely enable business as well as law enforcement to improve their common defense against cybercrime. In such a model, information like cyber-threat indicators, commonly exploited vulnerabilities and unexpected or particularly severe consequences are shared between industries and government, leading to the development of practices, technical expertise and data, and training tools. Such a model has been initiated through INTERPOL's arm focusing on cybercrime at its Global Complex for Innovation (IGCI) in Singapore. INTERPOL plays a unique role in assisting police in 190 member countries to identify and share intelligence leads, bridge information gaps and disrupt the organized networks behind a range of cybercrimes which are often interlinked. The privilege and advantage of INTERPOL lies in its cooperation framework with law enforcement agencies of member countries, as well as its secure global police communications network I-24/7.

Law enforcement agencies can also contribute reports on the outcome of prosecutions and relevant materials that results from prosecutions, helping business and government better to prepare for future events. Knowledge sharing of cybercrime vectors, vulnerabilities and consequences can help law enforcement draw up new and effective criminal investigations, partner with industry to identify potential criminal activity. While legal constraints and confidentiality requirements of law enforcement agencies would generally prevent sharing of investigative information during investigation and prosecution, sharing of outcomes of prosecution would have a beneficial and potentially deterrent effect.

Despite the challenges on sharing investigative information, joint operational taskforces are the way forward in apprehending perpetrators of cybercrime and allowing for as many companies and organizations as possible to take the necessary steps to improve detection, protection, response and recovery from cybercrime. Alongside the set-up of a global platform, the creation of regional and continental platform should be promoted as well. Information sharing platforms as well as joint taskforces can take different forms depending on regional habits and structures of organizations, law enforcement authorities and companies concerned.

(b) Several joint cooperation models for combating cybercrime exist on the regional and national levels. Europol's Joint Cybercrime Action Taskforce (J-CAT) at the European Cybercrime Centre in The Hague, and the Federal Bureau of Investigations National Cyber Investigative Joint Task Force (NCI-JTF) in Washington DC are examples of cooperation models for combating cybercrime. Each provides a multistakeholder solution to intelligence-gathering and investigation into criminal cyber activity, although each includes different complements of public and private sector participants. The National Cybersecurity and Communications Integration Center at the US Department of Homeland Security, the National Cyber-Forensics & Training Alliance (NCFTA) in Pittsburgh, Pennsylvania, and the network of Information Sharing and Analysis Centers (ISACs) in the United States are models of information-sharing platforms. These models bring together different groupings of law enforcement, the private sector and academia to mitigate and combat cyber threats.

Where the set-up of a global or regional/continental platforms might be more time-consuming, an immediate benefit can be achieved by promoting further registration with, and commitment to, the regional/industry platforms that already exist, and improving coordination among these platforms. In regions and industries where information-sharing and joint task forces do not exist, their creation needs to be promoted and supported.

Recommendation 3

3. Public and private sectors should seek to promote greater global adherence to, and coordination of, the rule of law relating to cybercrime. This includes:

(a) Public and private sectors should seek to promote the adoption of the Convention on Cybercrime 2001 (Budapest Convention) – at least the key principles on substantive law (Articles 1-9 of the convention).

(b) Participants of cooperation platforms should respect the rules generally admitted regarding the sharing of information as well as the rules related to mutual legal assistance treaties (MLATs) in force at the time of information-sharing.

(c) Public and private sectors should promote the adoption and harmonization of national laws that capture the spirit and key principles of the Convention on Cybercrime (2001).

Commentary

(a) Despite the numerous laws and regulations on cybercrime, there is no international law dedicated to cybercrime. The closest item that comes to an international law is the Council of Europe's Convention on Cybercrime (2001), otherwise known as the Budapest Convention. Accession to the Budapest Convention offers a standardized legal framework, in line with international standards, that governs criminal acts executed on computer networks as well as the ability of law enforcement to procure any crime-related evidence from computer networks. The benefits also extend to the private sector in that a global cybercrime law would grant the private sector greater legal certainty and, consequently, increased security and confidence in the governance of cyber issues. While this convention counts non-EU members as signatories as well, it is not yet global. It also has to be modernized therefore the Cybercrime Convention Committee has decided to explore possible solutions which focus on the following:

- Ameliorating judicial cooperation in order for mutual legal assistance to be more efficient. The Cybercrime Convention Committee issued an assessment report and recommendation which were adopted in December 2014
- Developing wider interpretation guidance on Article 18.1.b of the Budapest Convention which relates to the ability of authorities to submit data production orders
- Developing an additional protocol to the Budapest Convention to address shortcoming and grey areas, notably issues surrounding data access and/or ways of addressing technological developments
- Developing guidelines on cooperation between law enforcement and internet service providers with regard to provision of data

(b) To ensure legitimacy as well as widespread ethical and political acceptance, the activities outlined in Recommendations 1 and 2 must be practised within existing legal frameworks, which include the policies and best practices adopted in this domain. Also, the authorities should promote the implementation of MLATs and relevant conventions existing in this field.

(c) In the absence of a globally applicable law, and where ratification/adoption of key principles from the Budapest Convention are not, or cannot be achieved, efforts should be made nationally so that, where lacking, states can implement the necessary cybercrime laws. Several models of cybercrime legislation have been elaborated and could be promoted.

Recommendation 4

4. Public and private sectors should work towards greater mutual cooperation to build trust and create opportunities for discussion and resolution of issues related to cybercrime. This includes:

(a) Law-enforcement and the private sector having open and constructive discussion on current issues which could be obstacles to the implementation of Recommendations 1 to 3 above.

(b) Law-enforcement authorities and the private sector working to create incentives within their respective communities, enabling them to commit to Recommendations 1 to 3 above.

(c) Public and private sectors collaborating to promote and/or create capacity-building programmes.

Commentary

(a) Matters such as data access, data localization, data privacy and encryption are fervently debated issues among nations and between governments and industry. This causes a dilemma in the cooperation of public and private sectors (especially when the issues transcend borders) in tracking cybercrime and apprehending perpetrators. It should be noted that public security and civil liberties are not competing entities. While this quandary and the need for reconciliation in the existing gaps are recognized, it should not prevent more noteworthy public-private collaboration in the fight against cybercrime.

Recognizing the shortcomings of the Budapest Convention in this regard, the Council of Europe has established the Cloud Evidence Group to address issues related to criminal justice access to evidence stored on cloud servers and in foreign jurisdiction. The council is also exploring methods by which data issues can be resolved. These include the Assessment and Recommendations adopted in December 2014 by the Cybercrime Convention Committee (T-CY) aimed at ameliorating judicial cooperation. In its vocation as an international organization for public-private partnership, the World Economic Forum is ready to facilitate these discussions during the next steps of the project.

(b) Recommendations 1-3 can be achieved only with the right reasons, motivation and encouragement thus momentum and a call to action must be created within the said communities. Innovative forms of financial incentives should be developed and promoted to anchor and support companies which voluntarily engage in implementing Recommendations 1 to 5. Additional mechanisms for providing private industry with the incentive to cooperate with law enforcement and share sensitive information might also come, for example, in the form of liability protection. Information-sharing raises a number of concerns for corporations; not only do they expose themselves to reputational damage but also to criminal or civil liability. Any protection of this kind should not exempt a corporation from clear wrongdoing or lack of action but providing specific liability protection (such as the new Cybersecurity Information Sharing Act passed by Congress and signed by President Obama in December 2015) would encourage corporations to come forward with information on cyber threats.

(c) The international fight against cybercrime can be achieved only if the right tools and techniques are in place to do so. This includes ensuring that those charged with combating cybercrime possess the right expertise in cyber-related issues. Capacity-building which, for example, includes targeted training for law-enforcement, prosecutors and judges, is necessary to ensure they keep abreast of technological developments and have requisite knowledge and skills to deal with the constantly evolving cyber landscape.

Recommendation 5

Public and private sectors can engage in other initiatives, such as collective action, to enhance the impact of unilateral private sector action to combat cybercrime.

Commentary
Such actions could complement or temporarily substitute weak local laws and collaboration. This does not mean that governments should not promote the model of collective action or endorse its results. The World Economic Forum, as an international organization for public-private cooperation, might act as a facilitator in such collective enterprises. An example of such collective action is the World Bank Institute's anti-corruption-focused partnership with businesses and NGOs: "Fighting Corruption through Collective Action – A Guide for Business".

Support of Recommendations

In recognition of the importance of cybercrime and its impacts on both public security and business, I confirm my support of the World Economic Forum's efforts in this field and commend the Forum's "Recommendations for Public-Private Partnership against Cybercrime" as a positive step in garnering attention and creating the impetus for global public-private collaboration in the fight against cybercrime.

Signature, name, title/position, country/company

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org