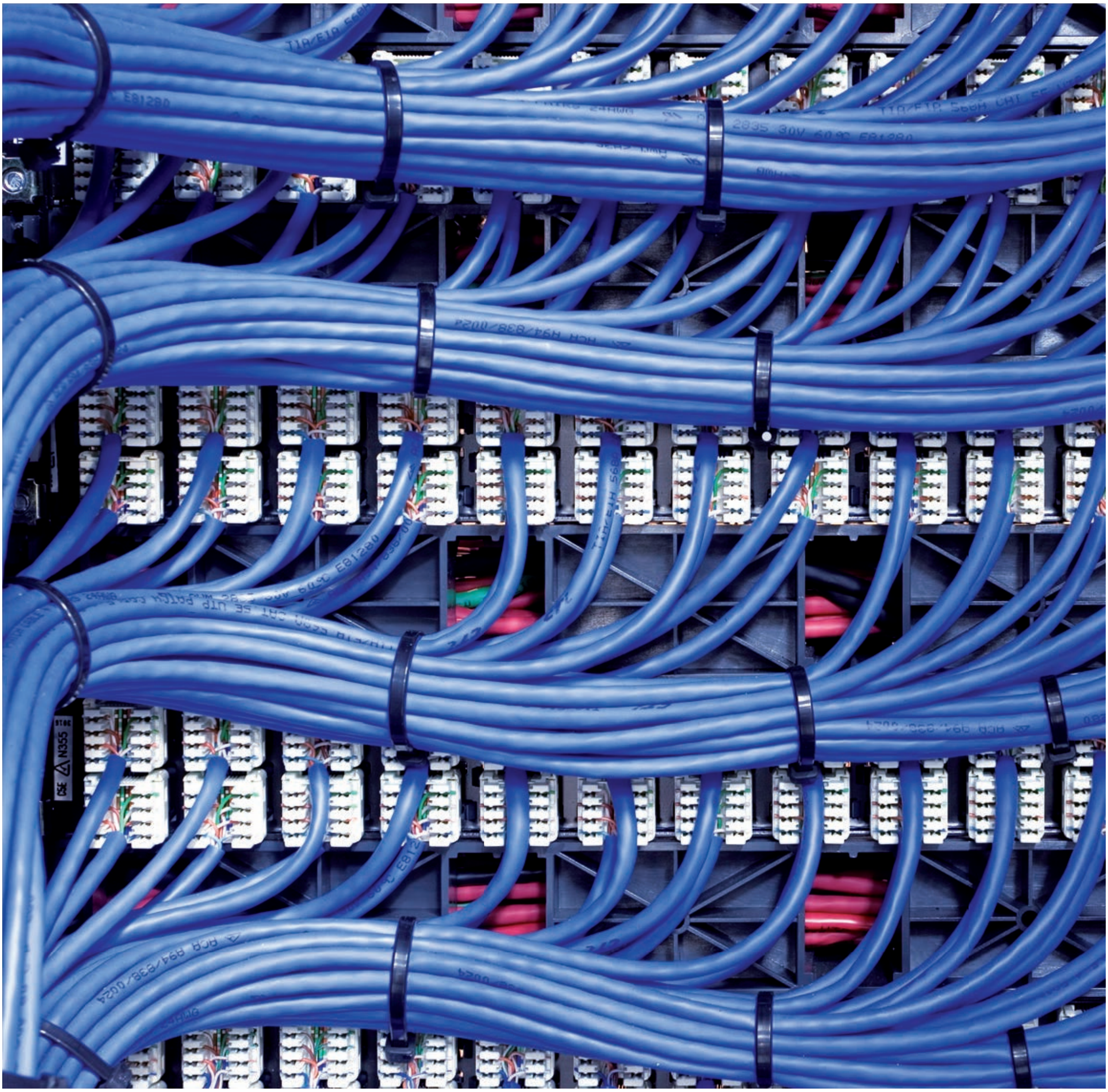
ESADE
Ramon Llull University
ESADEgeo-CENTER FOR GLOBAL ECONOMY AND GEOPOLITICS

ZURICH®

Risk Nexus

Global cyber governance: preparing for new business risks



Contents

Foreword

Javier Solana,
President, ESADEgeo-Center for
Global Economy and Geopolitics

Axel Lehmann

Axel P. Lehmann
Chief Risk Officer and Regional Chairman
of Europe, Middle East and Africa
Zurich Insurance Group

The process of globalization, the emergence of new powers, and the increasing relevance of non-state actors are creating a multipolar and interconnected world. In the international arena, political and ideological diversity among the most relevant parties, diffusion of power, and the impact of changing global economics have added complexity to the geopolitical landscape. Businesses now operate in a much more difficult, heterogeneous environment.

Global Cyber governance is one of the key challenges facing businesses. In view of the significance and complexity of the surrounding issues, ESADEgeo, a leading authority on global governance, and Zurich Insurance Group, a global insurer, have joined to offer insights into ways it might be improved.

We live in a world full of opportunities, but also risks. There is no better example of this than the relationship between information and communications technologies (ICTs) and cybersecurity. The cyber realm underpins almost all economic and societal activity – from finance to trade, information, energy and beyond. As Henry Kissinger suggests, technology is even challenging our traditional understanding of sovereignty and political order. Whether and how the risks associated with cyber technology are controlled will therefore have seismic consequences for all concerned. The 2014 Atlantic Council/ Zurich report, 'Beyond data breaches: global interconnections of cyber risk,' highlighted this correlation between risk and opportunity, noting in particular the highly systemic and cascading nature of cyber risk. According to the 2015 edition of the Global Risks report, the evolution of geopolitical tension into cyberspace and the impact of emerging technology are among the most important developments affecting the global risk landscape.

This report aims to provide a detailed study on the state of the global governance of cyber security. It assesses the current and evolving nature of cyber risk, examines the existing global governance framework, and proposes new paths to tackle the current disorder in cyberspace. The existing governance framework from the 20th century cannot be expected to respond sufficiently to a 21st century technology. This report contains a mixture of bold and pragmatic suggestions to resolve some of the more difficult issues we face.

The world needs a fluid and more comprehensive dialogue between business, politics and civil society to ensure the security of cyberspace. Developing an inclusive and reliable governance regime for the security of the cyber realm is a prerequisite to managing the risks and grasping the opportunities that emerging technology presents. It is therefore one of the critical tasks of our times: essential to protect economic growth, technical progress, political stability and social development. We look forward to working with others on this complex and exciting global challenge.

Executive summary

Section 1: Emerging technologies will fundamentally change the nature of cyber risk

Cyberspace has rapidly become essential to the daily life of individuals, governments and businesses. Yet with this exponential increase in activity comes the ease of use and access to data for malicious purposes. Cyber attacks are increasing in number, sophistication, scope and impact. In this context, cyber security is arguably the most salient non-traditional security issue on the global agenda.

Emerging technologies such as the Internet of Things will increase the complexity of networks. Other disruptive technologies, such as unmanned aerial vehicles, additive manufacturing (such as 3-D printing), new home appliances or autonomous vehicles may also shake up established business practices and create new security threats. Cyber risks will become increasingly interconnected with other global risks.[1] Much of this evolution is already apparent.

Companies in almost all sectors are exposed to cyber threats, with the potential for causing enormous damage in terms of reputation and physical losses, liabilities, and regulatory costs. Unchecked, growing cyber threats risk curtailing technical and economic development on a global scale.[2]

Section 2: An inadequate global cyber governance framework

Cyber attacks respect neither state nor organizational borders. A holistic and global approach to cyber governance is therefore vital. Despite some recent progress at the international and regional levels on norms and confidence-building measures (CBMs)[3], a comprehensive and functional regime of global cyber security governance is clearly lacking. In an effort to improve the situation, we undertook a detailed mapping of the rules, institutions, and procedures that form the current global cyber governance framework. This chapter summarizes the main conclusions of that work. An academic report containing this research in detail will be publicly available in the near future.

The current global cyber governance regime can be regarded as having three layers. First, there are the more technical aspects that facilitate the proper functioning of network systems. Global governance in this area is relatively effective, and is based on a multi-stakeholder model. At the other extreme of the spectrum are cyber warfare issues such as terrorism and espionage between states, or cyber attacks on critical infrastructure for political purposes. Here, effective global governance is lacking. Between these two extremes, we find the 'gray zone' – a sphere where the interests of industry, governments and individuals intersect. Issues addressed in this space include net neutrality, intellectual property rights, freedom of speech, non-state or criminal cyber attacks and data protection.

The 'gray zone' encompasses all international instruments that deal with cyber risks from a non-technical and non-military perspective. It is in this area, with its various global governance models and organizational cultures, that the international community can most effectively work to improve the current situation and facilitate the mitigation of cyber threats.

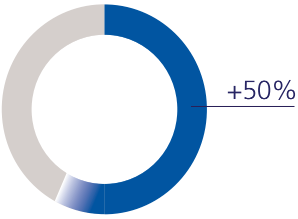
Our analysis has identified two key characteristics of global cyber governance: ideological differences and geopolitical tensions preclude strong and effective global governance institutions; and the current governance framework does not adequately reflect the global nature of cyberspace.

Authors' note: As with any pioneering research in a novel field, the samples and data available for this report have significant limitations. Many of the data points that would have been required are not publicly available, while others don´t even exist; that is, the relevant organizations do not compile the necessary information. Due to these limitations, the findings of the study should be treated with some caution. They are as accurate as the available information has allowed, but certainly not definitive. Yet they provide a valuable study of this topic and thus hopefully take the research a step forward to a point where it can be improved by future work.

Fast fact

Asia leads internet usage

Today more than 50% of the world's internet users are in Asia.



[1] Zurich Insurance Group/Atlantic Council (2014) 'Beyond Data Breaches: Global Interconnections of Cyber Risk,' Risk Nexus. Available at: http://www.zurich.com/internet/main/SiteCollectionDocuments/insight/risk-nexus-april-2014-en.pdf

[2] World Economic Forum (2015): 'Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats'. In collaboration with Deloitte, 2015, p.9.

[3] ICT for Peace, 'Baseline Review of ICT-Related Processes and Events: Implications for International and Regional Security', 2014, p.44.

Section 3: Toward a new governance framework: challenges and opportunities

Given the shortfalls in global cyber governance and the urgent need for effective risk mitigation, there are a number of recommendations that should be considered. In the absence of state consensus, we believe there is a role for the private sector to actively lobby for a set of guiding principles to overlay the global cyber governance framework. That governance should be global and inclusive in nature, based on a multi-stakeholder approach and flexible enough to adapt to rapidly-evolving challenges. The private sector should also take specific steps to mitigate cyber risk and enhance general resilience in the meantime, given the lack of effective global governance. Greater information-sharing will play a key role in developing the tools to achieve this, such as a well-functioning insurance market.

For policymakers, there are a number of steps that we believe, if taken, would allow major progress toward a more effective global cyber governance framework. Recommendations include:

- Strengthen 'fit for purpose' global institutions, which would include creating a G20 + 20 Cyber Stability Board and taking steps to isolate these institutions from geopolitical tensions.
- Consider creating a cyber alert system, based on the model of the World Health Organization (WHO).
- Enhance public-private cooperation, including dialogue and incentives for investment in cyber security.
- Seek to increase the representation of LDCs and civil society within the global governance framework.

Table 1: Summary of private sector and policymaker recommendations to improve global cyber governance

Recommendation	Proposed mechanism
Business	
Greater information-sharing to mitigate cyber risk.	Insurance industry via the CRO forum. Anonymized business loss reporting via private sector-led initiatives, e.g., FS-ISAC, public-private bodies e.g., ENISA.
Champion common values for global cyber governance in absence of governments' consensus.	Lobby through institutions, particularly privately-led initiatives, e.g., CRO forum and multi-stakeholder dialogue forums, such as WEF.
Take targeted actions to manage cyber risk.	Adopt SANS 20 Critical Security Controls. Further actions needed for larger organizations.
Enhance general resilience to cyber risk.	Built-in redundancy, incident response and business continuity planning, scenario planning and exercises.
Policymaker	
Strengthen those aspects of global governance that have worked properly and isolate them from geopolitical tensions.	Develop informal global cyber networks. Adopt a 'build it and they will come' approach.
Create a system-wide institution for incident response.	G20+20 Cyber Stability Board.
Enhance crisis management to deal with a potential systemic cyber crisis.	Cyber WHO (World Health Organization).
Seek greater public-private cooperation.	Incentivize alignment of public/private interests on cyber security.
Reinforce protection of critical information infrastructures.	Cyber stress tests.

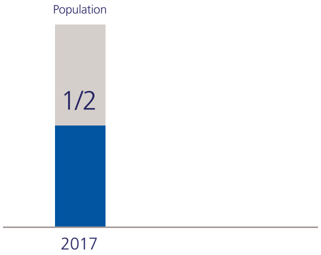
Section 1

Emerging technologies will fundamentally change the nature of cyber risks

Fast fact

The online population

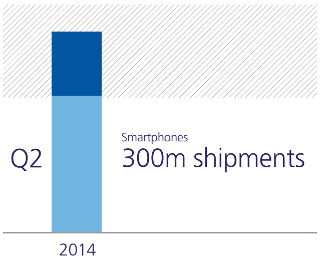
Around half of the world's population will be online by 2017.



Fast fact

Smartphone sales soar

According to the Worldwide Quarterly Mobile PhoneTracker, sales of smartphones exceeded 300 million units in shipments for the first time in Q2 2014.



1.1 Cyberspace – present and future

Information and communications technologies (ICTs) have become a central part of everyday life. Cyberspace has become the backbone of operations and communications for both businesses and governments. These technologies are a key factor fueling social and economic development, innovation and growth. Yet we are only at the beginning of a fundamental transformation. Over the coming years, new technologies such as big data, unmanned aerial vehicles, additive manufacturing, new home appliances or autonomous vehicles are likely to shake up established business practices, regulatory paradigms and even social norms.

The Internet of Things (IoT) – or what is considered by many as the next evolutionary stage, the Internet of Everything (IoE) – will increase networks' complexity. Any aspect of human life may become online-dependent and billions of physical objects with ICT systems will be interconnected. Cisco Systems believes that over a 10-year period to 2022, USD 14.4 trillion in value is at stake in connecting up what is now unconnected through the Internet of Everything.[4]

Around half of the world's population will be online in 2017, a figure already reached for mobile phone users. Mobile broadband is considered the fastest-growing technology in human history, affecting even the poorest and remoter areas of the planet.[5] According to the Worldwide Quarterly Mobile Phone Tracker, in the second quarter of 2014, sales of smartphones surpassed the 300-million unit shipments mark for the first time[6] and the International Telecommunication Union (ITU) forecasts that the number of networked devices will reach 25 billion by 2020.

While these new technologies have the potential to generate massive social and economic benefits, they do not come without risks. As the world becomes increasingly connected to, and dependent upon, cyberspace, the increasing vulnerability of cyber systems has set alarm bells ringing. For example, as cyber activity grows enormously, access and use of data for malicious purposes remains relatively easy. Despite the lack of reliable figures, there is a consensus in the cyber security community that attacks have increased in number, sophistication, scope and impact.[7] In the U.S. alone, the annual costs of cyber crime are estimated at USD 100 billion.[8] In this context, cyber risks have attracted significant attention and are a leading security issue on the global agenda. Individuals, governments, and the private sector are beginning to recognize the scale of the challenge. James Clapper, the U.S. Director of National Intelligence, stated in 2013 that cyber threats posed the most significant transnational threat to the United States.[9]

[4] John Chambers, 'Possibilities of The Internet of Everything Economy,' Cisco Blog, The Platform. 18 February 2013. Available at: http://blogs.cisco.com/news/the-possibilities-of-the-internet-of-everything-economy.

[5] Broadband Commission (2014) 'The State of Broadband 2014: Broadband for all.' ITU and UNESCO. Available at: http://www.broadbandcommission.org/Documents/reports/bb-annualreport2014.pdf

[6] The International Data Corporation (IDC) Worldwide Quarterly Mobile Phone Tracker.

[7] The Europol European Cybercrime Centre – EC3 (2014) 'The Internet Organised Crime Threat Assessment (iOCTA)'. Available at: https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf

[8] The Wall Street Journal, 'Annual U.S. Cybercrime Costs Estimated at $100 Billion,' 22 July 2013.

[9] U.S. Department of Defense (2013) 'Clapper Places Cyber at Top of Transnational Threat List.' Available at: http://www.defense.gov/news/newsarticle.aspx?id=119500

“Focus is increasingly shifting from defense to resilience.”

1.2 An environment favoring attackers

Cyber attacks take place in an environment which favors attackers. For example, because most cyber infrastructure was designed for openness and interoperability rather than security, offensive actions have an advantage over defensive actions. There are also lower barriers to criminal entry in cyberspace than in the physical world and a weak government monopoly on the use of force. This allows attackers with limited resources to carry out disruptive actions with considerable, and often unpredictable, outcomes. Such attacks may be difficult to attribute, with anonymity reinforced by darknets.[10] Moreover, it is difficult to assess the damage suffered by the target.

The introduction of new technologies often lacks necessary security elements. These include correct design, configuration, maintenance and management. New developments such as big data, wearable devices, augmented reality and artificial intelligence will increase the potential size, types and frequency of attacks.[11]

In addition, the BYOD[12] trend – whereby all devices tend to converge – will continue to reduce the separation between professional and recreational systems. This is worrying considering that mobile cyber crime is an extremely widespread phenomenon.[13] Cyber crime has revealed itself to be very lucrative, with recent estimates suggesting that the cyber black market can be more profitable than the illegal drug trade.[14] Thus, in recent years cyber crime has grown faster than hacktivism. While it is difficult to quantify the cost of global cyber crime and cyber espionage to the global economy, a publication by McAfee and the Center for Strategic and International Studies estimated the total cost of cyber crime at between USD 300 billion and USD 1 trillion, or 0.4 percent to 1.4 of global GDP.[15]

Box 1: Global cyber governance

The network of formal and informal institutions, mechanisms and processes that guide or restrict activities in cyberspace on a global or regional scale, thereby organising and articulating collective interests in cyberspace. This includes concrete cooperative problem-solving solutions negotiated by international bodies, governments, and non-state actors aiming to improve the management of cyber risks.

1.3 The changing nature of cyber risk

The rapid expansion of cyberspace is having a major impact on the nature of cyber risk – cyber threats are becoming increasingly interconnected with other global risks.

Much of this interconnectivity is already apparent. Companies in almost all industries are exposed to cyber threats with the potential for enormous damage in terms of reputation, physical losses, liabilities, and regulatory costs. At the same time, the distinctions between criminal and state-sponsored cyber-attacks on the one hand, and state or civilian targets on the other, have become blurred. There have already been well-publicized attacks on private firms that have been attributed to North Korea, among others. Elsewhere, conflict in the Ukraine is fuelling fears that western governments and private companies, including financial institutions, will become targets of Russian cyber attacks.

Box 2: Disruptive cyber events

A disruptive cyber event affects networks, systems, assets, and infrastructures of technology-dependent organizations and individuals. These events include, among others, malware, attacks on critical information infrastructures, and networked information systems, website defacement, espionage and extortion. It also includes unintentional mistakes, privacy policy violation, theft of intellectual property, online fraud, and denial of service attacks.

Massive cyber breaches at Sony, JPMorgan, Target, Home Depot, Albertsons, Dairy Queen and other corporations in recent years underscore the relevance of cyber security awareness for companies in the private sector. According to a report by the Ponemon Institute, 43 percent of U.S. enterprises suffered a data breach in 2013.[16] A 2010 study by Norton found that 65 percent of internet users globally have been a victim of some type of cyber crime.

While the cost of cyber incidents to businesses is difficult to quantify, a number of studies show that it is rising.[17]

[10] A virtual private network within the deep web where users only connect with trusted peers through technologies such as Tor, the Invisible Internet Project (I2P) and Freenet.

[11] The Europol European Cybercrime Centre – EC3 (2014) ‘The Internet Organised Crime Threat Assessment (iOCTA)’. Available at: https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf

[12] Bring your own device.

[13] Kaspersky Lab and Interpol (2014) ’Mobile Cyber Threats’. Available at: http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2014/10/report_mobile_cyberthreats_web.pdf

[14] Lillian Ablon, Martin C. Libicki, Andrea A. Golay (2014) ‘Markets for Cybercrime Tools and Stolen Data,’ RAND Corp. National Security Research Division and Juniper Networks. Available at: http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

[15] James Lewis, Stewart Baker. ‘The Economic Impact of Cybercrime and Cyber Espionage.’ McAfee, and The Center for Strategic and International Studies (CSIS). July 2013. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

[16] Ponemon Institute LLC (2014) ‘The Challenges of Cloud Information Governance: A Global Data Security Study’.

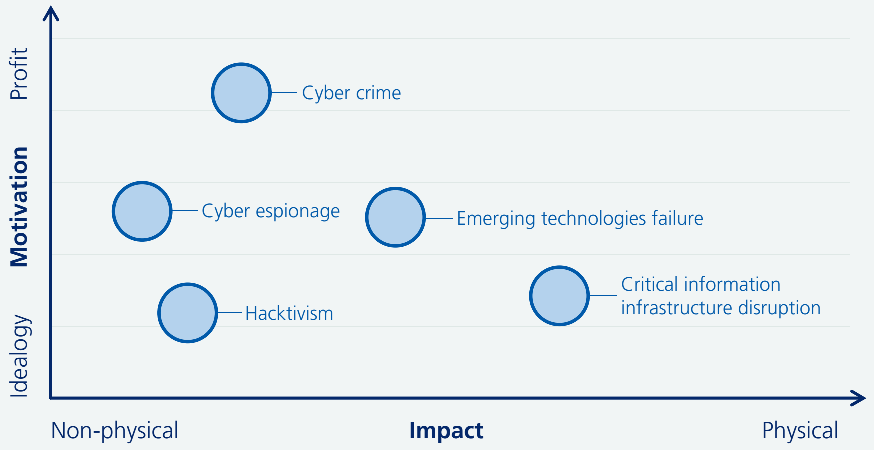
[17] Ponemon Institute LLC, sponsored by IBM (2014); 2014 Cost of Data Breach Study.

Increasing interconnectedness raises the potential for systemic and cascading cyber crisis, with real consequences for the economy.[18] For example, the management of critical infrastructures such as electricity grids, power plants, dams, water distribution systems, railway systems, oil refineries, pipelines, and chemical factories has significantly improved due to the development of industrial control systems (ICS). These command and control information systems are used to control, monitor, and support industrial processes and operations such as manufacturing, product handling, production, and distribution.[19] The most important subgroup of ICS comprises supervisory control and data acquisition (SCADA).[20] SCADA platforms are progressively more open, based on standard technologies, and interconnected. This has reduced costs and improved the overall quality of these systems. However, it has also increased their vulnerability to cyber attacks and made them easier to compromise, as the Stuxnet worm[21] in 2010 demonstrated.

Another crucial area of concern is the relationship between the financial sector and the cyber realm. The world's financial markets are interconnected. This makes the impact of a cyber attack potentially catastrophic. The first priority of cyber war games announced in January between the U.S. and UK was to test resilience of both nations' public and private financial institutions.[22]

As a result of growing interconnectedness, the potential for broad physical and economic consequences of cyber attacks is increasing. In order to assess these risks, different categories of cyber threats should be analyzed both in terms of their underlying motivations as well as potential impacts, as shown in Figure 1. While traditional cyber crime is mainly driven by profit motives of criminal organizations, growing geopolitical tensions may lead to a rise in ideologically-motivated attacks. Table 2 provides more details on the main threat categories.

Figure 1: Cyber risk landscape by motivation and impact



Source: ESADEgeo.

The increasing connectivity and complexity of cyber risk has led to a change of emphasis concerning mitigation – from a focus on defense to greater concern for system resilience. This includes strategies focused on detection, response, and recovery.[23, 24, 25] Priorities have shifted: it is no longer about avoiding all attacks, but about ensuring that systems can continue to operate, even after an attack, and can quickly recover.

[18] Zurich Insurance Group/Atlantic Council. See footnote 1.

[19] NIST (2009) Special Publication 800-53, App. B, Glossary.

[20] ENISA (2011) 'Protecting Industrial Control Systems. Recommendations for Europe and Member States.' Available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states

[21] A computer worm designed to target Siemens SCADA systems that attacked the Iranian nuclear facility at Natanz.

[22] http://www.bbc.com/news/uk-politics-30842669

[23] Clemente, D. (2013) 'Cyber Security and Global Interdependence: What Is Critical?' Chatham House. Executive summary available at: http://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/Executive%20Summary%20Cyber%20Security%20and%20Global%20Interdependence_0.pdf

[24] Zurich Insurance Group/Atlantic Council. See footnote 1.

[25] Georgia Institute of Technology (2014) 'Emerging Cyber Threats Report 2014.' Available at: http://www.gtsecuritysummit.com/2014Report.pdf

Table 2: Cyber risk landscape

	Description	Examples	Main damage	International organizations (IOs)
Hacktivism	Use of networked platforms to pursue an ideological goal or obtain notoriety. No (or limited) physical effect.	DDoS attacks, website and server disruption, DNS hijacking, cybersquatting.	Data compromise or exposure, operational shut down or slow down, damage to organizational assets.	INTERPOL, EC3, CEC (BC), ISF
Cyber espionage	Unauthorized network penetration to access information. Risks related to IPR. Financial or ideological motivation. Generally non-physical effects.	Spyware, data theft, extortion, advanced persistent threat (APT).	Intellectual property infringement, theft or breach of confidential information, loss or corruption of data.	INTERPOL, EC3, CEC (BC)
Cyber crime	Unauthorized network penetration to disrupt and damage systems, as well as stealing data, for financial gain. Mild physical effects.	Phishing, malware, APTs, viruses, worms, Trojans, spam, spoofing, ransomware, scareware, stolen devices, web-based attacks, adware, botnets, skimming, fast flux, spoofed apps.	Supply chain compromise, reputation damage, business interruption, online child sexual exploitation, identity theft, extortion, money laundering.	INTERPOL, EC3, FIRST, CEC (BC), ISF, NRO
Emerging technologies failure	Risks related to the introduction of new technologies. Generally significant physical effects.	Internet of things, embedded medical devices, driverless cars, cloud systems.	Integrity, availability, performance and security of connected devices.	ICANN, IETF, ISOC, IEEE, ENISA, W3C, IEC, ISO
Critical information infrastructures disruption	Risks from disruptions to infrastructure. Attacks to SCADA systems. Strong physical effects.	Submarine cables, smart grid, electricity, financial systems.	Destruction, damage, or disruption of critical information infrastructures.	ENISA, ITU, UN-GGE
Cyber warfare	Risks related to the use of networks by nation states or related groups to destroy or damage ICT systems. Targeting a nation's private sector may be a focus.	International conflicts.	Destruction, damage, or disruption of defense networked systems.	

> “Besides maintaining internal security, businesses need to work with the public sector.”

1.4 The impact of global cyber governance on business

An effective governance framework is a necessary pre-condition for society to reap the massive benefits of new technologies. Businesses will rely on effective global governance of the internet to support their investments in the digital economy and related new business models to benefit their consumers.

However, the existing global cyber governance framework is ill-prepared for the associated threats. If left unchecked, cyber risks will have profound consequences for businesses that increasingly rely on cyberspace. Such impacts will stretch well beyond data breaches and include theft of intellectual property, threats to global supply chains, failure of critical infrastructures and, as argued by Zurich Insurance Group and the Atlantic Council, even systemic cyber crises.[26] Uncertainty around global cyber governance thus risks curtailing innovation and economic growth on a global scale.[27]

Businesses have a clear interest in ensuring a safe, open and reliable internet. As well as mitigating the risks at a global level, an effective cyber governance framework will also enhance the ability of the insurance industry to provide cost-efficient insurance propositions to its customers to cover residual risks.

In addition to maintaining the security of their networks and infrastructures, businesses should therefore actively work together with the public sector to address the broader issues to promote a safe, open and reliable internet.

Box 3: New challenges for the financial sector

A crucial area of concern in the coming years will be the relationship between the financial sector and the cyber realm. Financial markets are globally interconnected, which makes the impact of cybercrime potentially catastrophic. According to John E. Savage, a fellow of the IEEE, the undersea cable system captures more than 95 percent of the global internet traffic including around USD 10 billion in financial transactions per day.[28] The cyber resilience of the financial system is a fundamental goal for preventing economic loss, reputational damage, or a massive loss of confidence. Several experts point out that underestimating cyber threats in the financial sector could lead to a ‘black swan’ event. A triggering cyber event could lead to knock-on shocks, similar to the ‘Lehman moment’ in 2008, due to the systemic character of the financial sector. According to Verizon, in 2013 the financial sector suffered the third-largest number of security incidents – behind only the public sector and the technology industry. Moreover, the proposed alternative to SWIFT, led by Russia and China, also raises questions about the future of online financial transactions.

A recent breach discovered by JPMorgan Chase affecting 83 million bank accounts is a clear example that the risk of cyber-attack in the financial sector cannot be underestimated.[29] Recurring failures in high-speed trading systems, over-the-counter (OTC) transactions, or errors in the purchase of shares in stock markets (fat fingers) are a source of concern, potentially threatening the stability of the electronically-controlled financial system, such as in the May 2010 flash crash. In addition, a cloud service provider failure could trigger unexpected impacts.

Financial transactions and e-commerce represent the e-version of trade globalization. This is evident in today’s interdependent global economy. It is becoming more common for third parties such as service providers or subcontractors to access company data. In future scenarios of global supply chains, the vulnerability of data will facilitate the exploitation of third parties’ security flaws and involve the entire chain. Most subcontractors do not report or cooperate in the event of discovering a breach, and therefore the integrity of data supply chains is a growing concern for cyber security. It is therefore necessary to develop global governance in which the vast majority of relevant actors share interests.

[26] Zurich Insurance Group/Atlantic Council. See footnote 1.

[27] World Economic Forum (2015): ‘Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats’. In collaboration with Deloitte, 2015, p.9.

[28] ‘Experts: Cyber-war threatens U.S. security’. Providence Journal, 18 June 2013. http://www.providencejournal.com/breaking-news/content/20130618-experts-cyber-war-threatens-u.s.-security.ece?template=printart

[29] ‘JPMorgan hack exposed data of 83 million, among biggest breaches in history’. Reuters, 2 October 2014. http://www.reuters.com/article/2014/10/03/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141003

Section 2

An inadequate global cyber governance framework

There is still no overarching global framework for cyber security."

The increasing interconnectivity and aggregation of risks in a complex system such as cyberspace renders borders of organizations and states irrelevant. Attacks that originate in one location may affect multiple jurisdictions. A holistic and global approach to cyber risk is thus vital. Despite some recent progress at the international and regional levels on norms and confidence-building measures[30] (CBMs), a comprehensive and functional regime of global cyber security governance is clearly lacking.

In recent years, several international, regional, technical, and informal bodies have addressed the cyber-security issue. These include the United Nations, Council of Europe (CoE), the Organisation for Economic Co-operation and Development (OECD), INTERPOL, the Group of 20 (G-20), Group of Eight (G-8), and the Organization for Security and Co-operation in Europe (OSCE).

In order to assess the effectiveness of the existing cyber governance framework, we undertook a detailed mapping of the rules, institutions, and procedures that govern the relationships among the different agents operating in this sphere. This chapter summarizes the main conclusions from this work.

An academic report containing this research in detail will be publicly available in the near future.

2.1 Three layers of cyber governance

The current global governance of cyber risks can be viewed as comprising three layers.

First, there is the layer of more technical aspects that help network systems to function properly, by ensuring that all the infrastructure and devices constituting the internet can talk to each other. On this level, global governance is largely effective – following a multi-stakeholder model based on a loose, bottom-up consensus. These actors are mainly interested in maintaining cyberspace as an open, cohesive place to secure connectivity, manage infrastructure in the right way and enforce cyber security.

In this category, the actors tend to understand cyber security as a shared responsibility, one in which each network is responsible for its own security and contributes to the overall security of the system. This encourages a sense of collective stewardship and puts the emphasis on confidence-building and international cooperation to address cyber risks. This approach has been reinforced by the increasing interconnectivity and hyperconnectivity of cyberspace, which creates new vulnerabilities and opportunities for disruptive attacks.

Our research suggests that the technical layer is where the bulk of the financial resources are allocated: Technical mechanisms, e.g., for standard setting and number management, seem to have larger budgets than other mechanisms.

[30] ICT for Peace, 'Baseline Review of ICT-Related Processes and Events: Implications for International and Regional Security', 2014. p.44

Table 3: Cyber governance subsets

Cyber governance subset	Main relation
Technical governance	Private to private (and IOs)
Gray zone	Private to private (and IOs) Private to government (and IOs) Government to government (and IOs)
Cyber warfare	Government to government

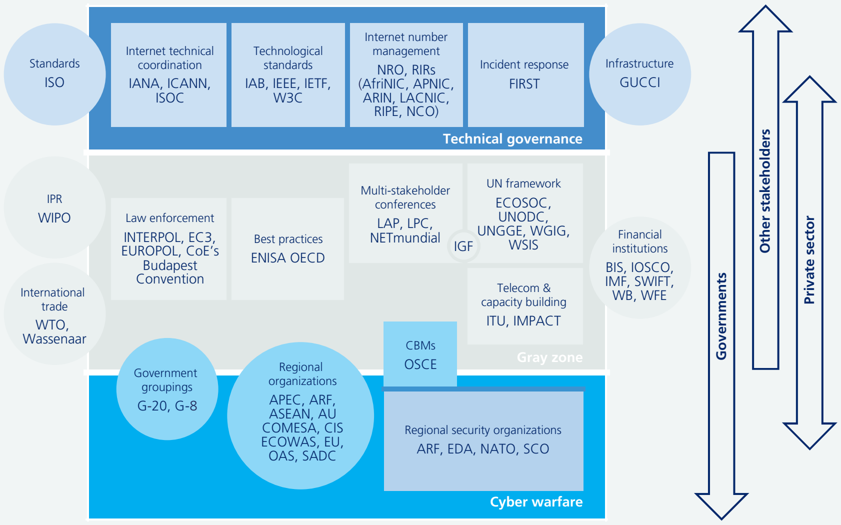
Cyber warfare represents the other end of the spectrum, and includes issues relating to state-sponsored cyber attack, espionage between states, and cyber attacks on critical infrastructure for political purposes. Here, a global governance framework is absent, achieving mutual understanding is progressively more difficult, and the role that international organizations play is far from effective. The bilateral method prevails between governments, and no change is expected in the medium term due to the sensitive political nature of homeland security, content control, or privacy protection involving individual governments. The dual role of governments, both in terms of national defense and as perpetrators, has eroded trust and renders the agreement on common norms difficult.

There is no transparency about the level of resources that flow into these efforts, as the entities involved do not publicly report their budgets.

Between these two extremes is a 'gray zone' – a more diffuse realm where the interests of industry, governments, and individual citizens intersect. Issues addressed in this space include intellectual property rights, cyber attacks by non-state actors on individuals, criminal activity and data protection. This subset of governance encompasses all international instruments that deal with cyber risks from a non-technical and non-military perspective. The international institutions within this group are thus unsurprisingly very diverse in nature and purpose. Neither the bilateral approach, nor a multi-stakeholder model, dominates. International institutions responsible for mitigating the risks of this subset of cyber governance range from state-centric multilateral formal institutions, regulatory mechanisms, and non-formal forums, to private organizations that influence best practices on cyber security. In the gray zone, international institutions that are not exclusively dedicated to cyberspace-related issues have considerable influence.

It is in this gray zone, with its complex set of governance models and organizational cultures, that the international community can most significantly improve cyber governance with the aim of mitigating cyberthreats (see Figure 2).

Figure 2: Global cyber governance institutions



Source: ESADEgeo.

> Ideological and geopolitical friction has led to incomplete memberships in many governance institutions.”

2.2 Key characteristics of global and regional governance capabilities

According to our research, the following points comprise the key characteristics of the current global cyber governance framework:

2.2.1 Ideological differences preclude strong and effective institutions

Given cultural, ideological and political differences across regions and countries, there exists no unanimously-accepted set of values to clearly guide global cyber governance. The revelations of large-scale surveillance programs have exacerbated the problem, leading to an erosion of trust and making it even more difficult for countries to agree on a common set of norms.

One group would prefer a ‘world government’ of cyberspace and an intergovernmental modus operandi.

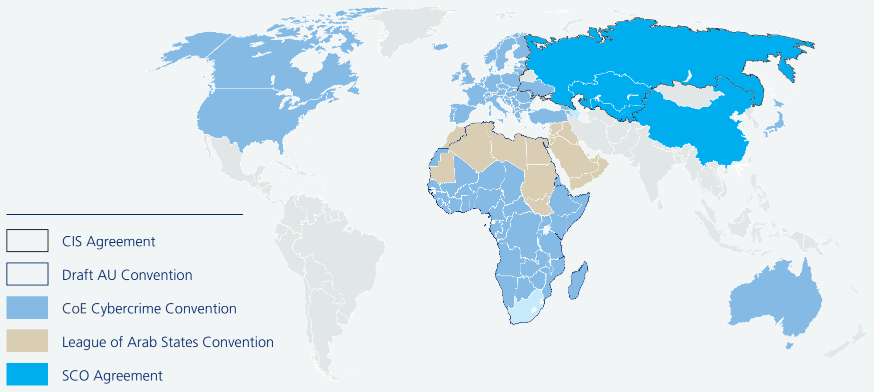
China, Russia and most Arab states are proponents of this model, supporting greater governmental control over cyberspace.

In the opposite camp, the U.S., EU and Japan, and some other highly-developed industrial nations defend the current multi-stakeholder system where non-governmental institutions play a fundamental role. Among the non-aligned are the ‘swing states’ led by the IBSA Dialogue Forum (India, Brazil, South Africa).[31]

The growing importance of cyberspace and its related threats has led to a proliferation of international initiatives to discuss policy, non-binding principles, best practices, and standards to mitigate cyber risk. In this category, the UN framework plays a key role, with forums and bodies such as the UN Group of Governmental Experts (GGE), the World Summit on the Information Society (WSIS), or the Internet Governance Forum (IGF).

Our research found that while some institutions are working well, the ideological and geopolitical friction between states has led to incomplete memberships and limited effectiveness in many global cyber governance institutions. UN-dependent forums, for example, tend to lean toward state sovereignty and the principle of non-interference in internal affairs. This makes it much more difficult to reach agreements or even a basic consensus. It is especially noteworthy that the three main poles on cyber security issues (the U.S., China, and Russia) rarely coincide in terms of their membership in non-UN-sponsored initiatives. The governments of these three countries only agree to membership of organizations that are not specifically focused on cyber security – such as regional security mechanisms and G-groupings: OSCE (the U.S. and Russia); the Shanghai Cooperation Organisation (SCO) (China and Russia); G-8 (the U.S. and Russia); and G-20 (the U.S., China and Russia). The lack of bodies in which the governments of the cyber powers are simultaneously present becomes clearer if we widen the focus to include the EU, Iran, and Israel. Nor is there any convergence in the matter of legal instruments. After analyzing the memberships of the international legal instruments that govern the cyber domain, we have concluded that no legal convention or agreement has been signed by all three major states (see Figure 3).

Figure 3: International and regional legal instruments relating to cyberspace



Source: UNODC Comprehensive Study on Cybercrime, 2013.

[31] Maurer, T. & Morgus, R. (2014) ‘Tipping the scale: an analysis of global swing states in the internet governance debate,’ Internet Governance Papers, CIGI.

Box 4: Forums

Stand-alone forums tend to be process-oriented initiatives. They aspire to represent all actors affected by the cyber sphere, especially civil society and the broad public. These multi-stakeholder forums emphasize a bottom-up approach, consensus-building, and discussions among all parties on equal footing. The boards of forums do not make decisions, hence have no decision-making mechanisms.

The Internet Governance Forum (IGF), is an example of such a grouping. It is an open forum without permanent members, which has a small supporting secretariat in Geneva and no negotiated outcomes. The Forum's mandate is to "discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet." For its part, the World Conference on International Telecommunications (WCIT), a UN treaty conference held in Dubai in 2012, discussed International Telecommunication Regulations (ITRs), network security, and the future of the cyber governance.

There are other significant forums: the London Process on Cyberspace (LPC) established in 2011 by the British Foreign & Commonwealth Office; NETmundial (the global multi-stakeholder meeting on the future of internet governance) that kicked in on April 2014 in São Paulo under the lead of the Brazilian Internet Steering Committee and 1net, a multi-stakeholder forum on internet governance.[32]

Box 5: Formal international institutions

The ITU, one of the oldest intergovernmental organizations (IGOs), is a good example of a formal international institution within the global cyber governance framework. It was founded in Paris in 1865 as the International Telegraph Union. Traditionally its responsibilities have included allocating radio spectrum, regulating international telecommunications and managing satellite orbits. With the expansion of information and communications technologies (ICTs), the ITU today plays a central role in developing standards and security frameworks, organizing diverse forums, facilitating access to resources for states, implementing multiple projects and initiatives, and assisting UN agencies. The ITU launched its Global Cybersecurity Agenda (GCA)[33] in 2007. Under this framework, the ITU established the High-Level Expert Group (HLEG) on cyber security, launched the Child Online Protection (COP) initiative and supported cyber security capacity-building in least-developed countries (LDCs). The ITU International Multilateral Partnership Against Cyber Threats (ITU-IMPACT) carried out assessments on Computer Incident Response Teams (CIRTs) in more than 50 countries to serve as a national focal point for improving the coordination of incident response to cyber attacks.

Our analysis shows an increasing interest in the multilateral governance of cyber security among formal international institutions. The scope of cyber issues managed by these organizations extends beyond technical aspects to sensitive and divisive issues such as espionage, privacy, content control, and human rights. This makes it harder to reach agreements within institutions with a broader mandate that include cyber governance programs, than in the more specialized institutions.

In the medium-term, less formal institutions, such as the G-20 and regional organisations such as the OSCE, the Asia-Pacific Economic Cooperation (APEC), the Association of Southeast Asian Nations (ASEAN), and the Organization of American States (OAS), will be called upon to play a greater role in the governance of cyber security.

[32] For an overview of private sector initiatives, see Box 7.

[33] ITU (2007) Global Cybersecurity Agenda. Available at: http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

“No legal convention has been signed by all three major states.”

Box 6: International agreements

The Council of Europe (COE) Budapest Convention on Cybercrime[34] adopted on November 8, 2001, is the most notable initiative and the first treaty addressing cyber crime in the international arena. As of February 2015 it had been signed by 53 states, including six non-COE countries.[35] A far greater number of countries are basing their own national cyber crime legislation on the Budapest Convention, which focuses on international criminal cooperation in the field of computer and network security.

Its main objectives are to harmonize domestic law and facilitate international cooperation. On March 1, 2006, the Additional Protocol to the Convention on Cybercrime came into force. Although the Budapest Convention provides regular consultations (at least once a year) in the Cybercrime Convention Committee (‘T-CY’), most analysts believe the Budapest Convention needs to be updated to make it more responsive to new threats and challenges.

[34] Council of Europe (2001) Convention on Cybercrime. Available at: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[35] The non-Council of Europe states that have ratified the treaty are Australia, Dominican Republic, Japan, Mauritius, Panama and the US (March 2014).

2.2.2 The current governance framework does not adequately reflect the global nature of cyberspace

Cyberspace is a truly global phenomenon. However, our research finds that the overall governance framework is primarily focused on Europe and North America. Only two global mechanisms are based outside these two regions – IMPACT and the INTERPOL Global Complex for Innovation (INTERPOL GCI) – both based in Southeast Asia. Interestingly, both of these mechanisms are security-related. In addition, the ASEAN Regional Forum has been active in the field of confidence-building measures (CBMs) in cyberspace.

The wealthiest governance mechanisms seem to be located in the west, most notably in the U.S. Some European cities with a diplomatic tradition, such as Geneva and The Hague, also account for a substantial portion of the total. Latin America and Africa usually host only regional institutional mechanisms with technical and coordination roles, which operate on small budgets.

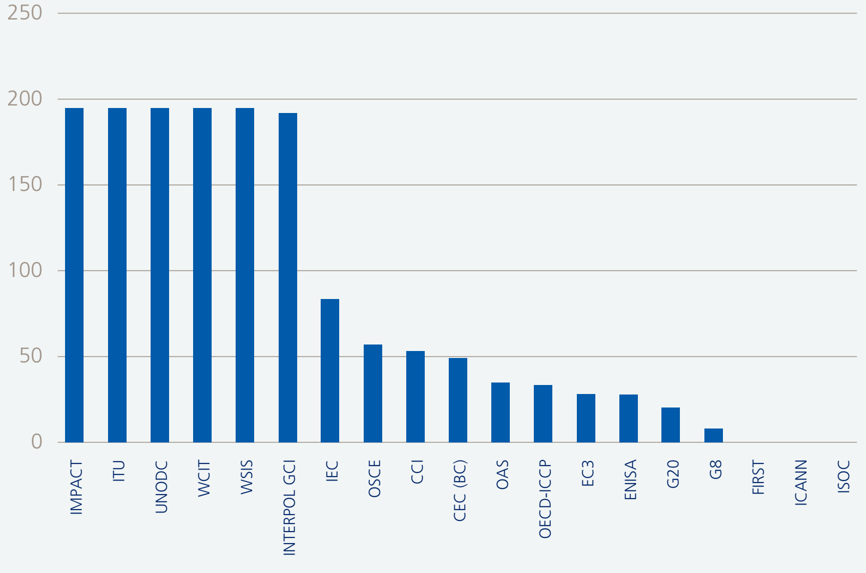
Technical governance, while more effective than other layers, is far from universal, particularly in the area of incident response. The Forum for Incident Response and Security Teams (FIRST), an international confederation of 305 computer emergency response teams (CERTs), is essential in this field. Yet it operates in just 66 countries.

The number of internet users in least-developed countries (LDCs) surpassed that of industrialized countries in 2005.[36] Today more than 50 percent of internet users worldwide are in Asia. This reality, coupled with the projections of an explosive growth in internet users in emerging economies, means non-western countries will need to increase their participation in governance of cyberspace to construct an effective global framework.

Of special interest are the memberships of international institutions analyzed in this chapter (see Figure 4). We looked at how cyber governance organizations are connected to member states. In this way, we could identify the core institutional mechanisms of the cyber security governance system, and the central states within this universe. Based on membership of the organizations we analyzed, there seems to be a core group led by the UN framework.

The countries that are members of a larger number of institutions are clearly western or, to a lesser extent, countries such as Japan, South Korea and Mexico. The rest of the Asian and Latin American countries, in their approach to cyber security, fall somewhere between the group just cited, and another group that includes post-Soviet states, African countries and Arab nations, which are located on the periphery.

Figure 4: Member states of bodies analyzed
State membership/member numbers



Source: ESADEgeo.

[36] UNODC, The Globalization of Crime, 2010.

Section 3

Toward a new governance framework: challenges and opportunities

> Both the private sector and policymakers can take specific measures to improve cyber governance.”

3.1 The current cyber disorder

As cyber security has gained prominence on the agenda, some governments are becoming more involved in shaping policy. With cyber security issues traditionally the domain of technicians, businesses, and the military, this government involvement is having a significant impact on various international initiatives. A number of governments are creating and strengthening cyber security teams within departments overseeing foreign affairs. Diplomats are being called on to play a major role in these discussions.

The downside of this approach, as discussed in the previous chapter, is that this is likely to lead to cyber security becoming more politicized. In a multi-polar world where the major powers do not always share common values, political tensions may derail collective efforts to create a secure cyberspace.

A fundamental problem lies in the dual role of government, both as defenders against foreign intrusions as well as perpetrators. An increasing number of countries are building cyber offense capability, resulting in a new form of arms race. Often, the need for offensive cyber capabilities is motivated by the importance of deterrence and preemptive cyber defense.

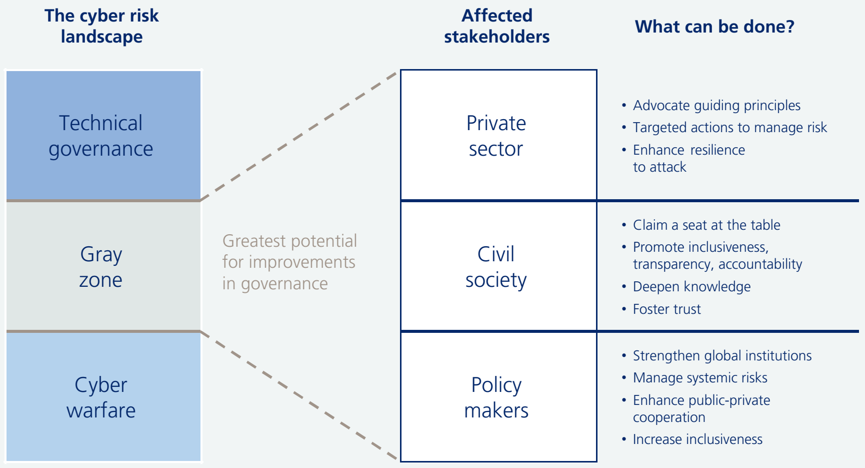
Part of the problem is mistrust among key players in the global cyber governance debate. The prevalence of U.S. companies in cyber technologies, for example, leads some to argue that the U.S. has ‘stewardship’ of cyberspace. Such mistrust not only affects interstate relations but also hinders real mutual trust between companies and states: Several companies from emerging economies (many of which are state-owned enterprises) maintain strong ties with their governments. Companies from developed economies also work closely with their governments.

Common tools to manage cyber threats that are already often lacking could get scarcer in coming years, making the situation worse. Concerns over surveillance programs have soured cyber-security relations between the U.S., Russia and China. Meanwhile,the EU and Brazil have announced their intention to deploy a USD 185 million undersea fiber-optic cable between Lisbon and Fortaleza to circumvent third-party surveillance.

Such a political approach may lead to ‘data nationalism.’ This would result in fragmentation and filtering of internet traffic at borders, confirming the fear of a cyberspace ‘Balkanization.’ Information protectionism of this kind would imply a scenario in which governments protect interests, close their own national systems, and create a restricted cyberspace that slows technological development and, in the end, undermines overall cyber security. Turkey and Iran have already passed laws to restrict internet traffic and telecommunications; other governments such as Hungary intend to follow this path. Some internet service providers (ISPs), led by the European Telecommunications Network Operators’ Association (ETNO) and some African nations, have proposed a ‘sending party pays’ system at the WCIT-12 that, if approved, would undermine the openness of the internet.

This state of disorder is particularly troublesome as the debate concerning the cyberspace global governance model heats up. Strong and concrete actions by both the private sector and policymakers are therefore needed to improve the global cyber governance framework.

Figure 5: Improving cyber governance: overview


The cyber risk landscape
Affected stakeholders
What can be done?
Technical governance
Gray zone
Cyber warfare
Greatest potential for improvements in governance
Private sector
• Advocate guiding principles
• Targeted actions to manage risk
• Enhance resilience to attack
Civil society
• Claim a seat at the table
• Promote inclusiveness, transparency, accountability
• Deepen knowledge
• Foster trust
Policy makers
• Strengthen global institutions
• Manage systemic risks
• Enhance public-private cooperation
• Increase inclusiveness

Source: Zurich Insurance Group.

3.2 Actions for the private sector

3.2.1 Champion common values

With geopolitical and ideological tension precluding any consensus among governments, we believe the private sector has a role to play when it comes to encouraging common values for cyberspace. The private sector should advocate the following three guiding principles for a global cyber governance framework to ensure a secure, resilient and open global cyberspace:

- An effective cyber governance framework must be global.
- The global cyber governance framework must be inclusive and based on a multi-stakeholder approach.
- The global cyber governance framework must be sufficiently flexible to adapt to ever-changing threats.

While a comprehensive regime of cyber governance would allow businesses to better manage cyber risks, it is clear from the findings of Chapter 2 that such a framework is not within reach in the foreseeable future.

In the absence of such a framework, businesses should take steps to protect themselves from emerging cyber threats.

3.2.2 Share information to mitigate cyber risk (see also Box 7)

Increased information-sharing is key toward being able to better understand, quantify and protect against cyber risks.

The insurance industry, through the Chief Risk Officers' Forum, is currently establishing infrastructure to better capture statistical cyber risk and loss data, and create common classifications of cyber risk. Along with common cyber reporting standards, these steps are the basis of a well-functioning cyber insurance market.

Businesses can also help by sharing their cyber attack experiences and loss information. However, concern in the private sector that failures or breaches of information could become public and damage reputations poses a major barrier to increased information sharing.

Data anonymity is therefore crucial. As the CRO Forum suggests, a cyber-risk database could be modelled on existing loss databases (e.g., those that exist for operational risks). The anonymity of such databases encourages events to be reported.

In the U.S., the Department of Homeland Security has initiated a working group, together with insurers, brokers, and company chief information security officers, to explore setting up a repository of information pertaining to breaches. The U.S. is considering limiting liability for those companies that share information.

> By sharing information the private sector can better understand and protect against cyber risks.”

3.2.3 Risk management

The Internet of Everything will bring businesses huge opportunities. At the same time, the associated risks are daunting. A comprehensive cyber governance regime would allow businesses to better manage these risks. But based on the findings of this report, achieving such a framework in the short-term is out of reach.

Businesses should take steps to protect themselves from emerging cyber threats. The 2014 report ‘Beyond Data Breaches: global interconnections of cyber risk’ by the Atlantic Council and Zurich Insurance Group[37] included basic recommendations for measures that smaller and larger businesses can take. It also provided recommendations to enhance general resilience against cyber attacks for companies of all sizes.

Basic measures

Regardless of the size of the organization, a relatively small number of actions can protect against most cyber risks. These actions are often quite simple and have not changed much over the past years; but one reason cyberspace remains so pervasively insecure is that so many organizations fail to implement them. Different groups of computer security experts have slightly different lists, but they generally overlap; the best known are the SANS 20 Critical Security Controls. The Council on Cybersecurity is pushing these 20 controls, especially the ‘First Five Quick Wins’ as follows:

- Application whitelisting.
- Use standard secure system configurations.
- Patch application software within 48 hours.
- Patch system software within 48 hours.
- Reduce the number of users with administrative privileges.

Advanced measures

Larger, more sophisticated organizations have the capability to engage in more advanced cyber risk management and should go well beyond the 20 Critical Security Controls.

Push out risk horizon: Advanced organizations should expand their view of cyber risk management to include counterparties, contract and outsourcing agreements, and upstream infrastructure. Each of these can be at least partially controlled by measures such as in-depth site visits and audits. Some technical tools will also increase awareness outside a company’s own perimeters.

Cyber insurance: With cyber insurance, companies can transfer cyber risks, especially third-party risks associated with data breaches or business interruptions. As more companies become involved and more products become available, this option is increasingly recommended to all companies, not just ‘advanced’ ones.

Demand more resilient and secure standards and products: Organizations with particular heft can push key vendors and standards organizations to incorporate more security and resilience, which can have a significant impact.

Board-level risk management: Boards need to become smarter on cyber risks, include a broad view of global aggregations of cyber risk in their risk registers, hold executives to account, and move away from a checklist/audit perspective.

[37] Zurich Insurance Group/Atlantic Council. See footnote 1.

3.2.4 Resilience

Unfortunately, one cannot hope that steps to protect against cyber risk will be completely successful. These disruptions will be of such frequency and intensity that most organizations will have to face them in the same way that they deal with natural disasters. Too much of this type of risk will be external, complex, and interdependent. Companies' main hope is therefore resilience – the ability to bounce back from disruptions to make these interruptions as short, and with as limited an impact, as possible.

Redundancy: A resilient organization needs redundant power and telecommunications suppliers, alternate ISPs connected to different peering points, and work-arounds with little reliance on IT to provide alternatives during internet disruptions.

Incident response and business continuity planning: Having trained teams ready to respond when the worst happens is an advantage that is often overlooked. The best teams have a comprehensive understanding of an organization's various business lines, and its most business-critical and time-sensitive information and systems.

Scenario planning and exercises: The best organizations examine the most likely and most dangerous cyber risks and exercise their security and response teams, as well as their corporate executives and boards, to build muscle memory for responding to incidents. Seize the opportunity that each crisis provides to create 'teachable moments' for responders and executives.

Risk dialogue: Given the rapidly evolving and increasingly serious potential impacts of cyber risk, it is important that businesses and the insurance industry maintain a regular dialogue. Such dialogue would help to inform businesses about the latest developments so that they can create awareness throughout their organizations. A dialogue would also allow businesses and insurers to create innovative, bilateral steps to mitigate against developing threats.

Box 7: Specific private-sector initiatives to close the cyber governance gap

Given the relevance of cyber governance to the business environment, the private sector has launched an increasing number of initiatives and activities to support efforts to close the governance gap. This box provides a selective, non-exhaustive overview of some key initiatives.

Establish norms

The World Economic Forum has launched a multi-year strategic initiative to bring together leaders from the public and private sectors with civil society leaders and the technical community to address overarching issues of global internet governance, which augment expert discussions within the Internet Governance Forum.

A number of companies, predominantly from the technology sector, have been promoting norms for the cyber space. Microsoft, for example, has informally proposed a set of norms to govern the internet. Global companies beyond the technology sector should consider joining efforts to promote norms as a foundation for an open, safe and resilient internet.

Better statistics and data

The Chief Risk Officers' Forum, whose members are executives in large, multinational insurance companies, has launched an initiative to create a foundation to better capture statistical cyber risk and loss data. Establishing common cyber reporting standards and practices for coding and classifying cyber risks not only will facilitate information-sharing, risk identification and assessment, but also form the basis of a properly-functioning cyber insurance market.

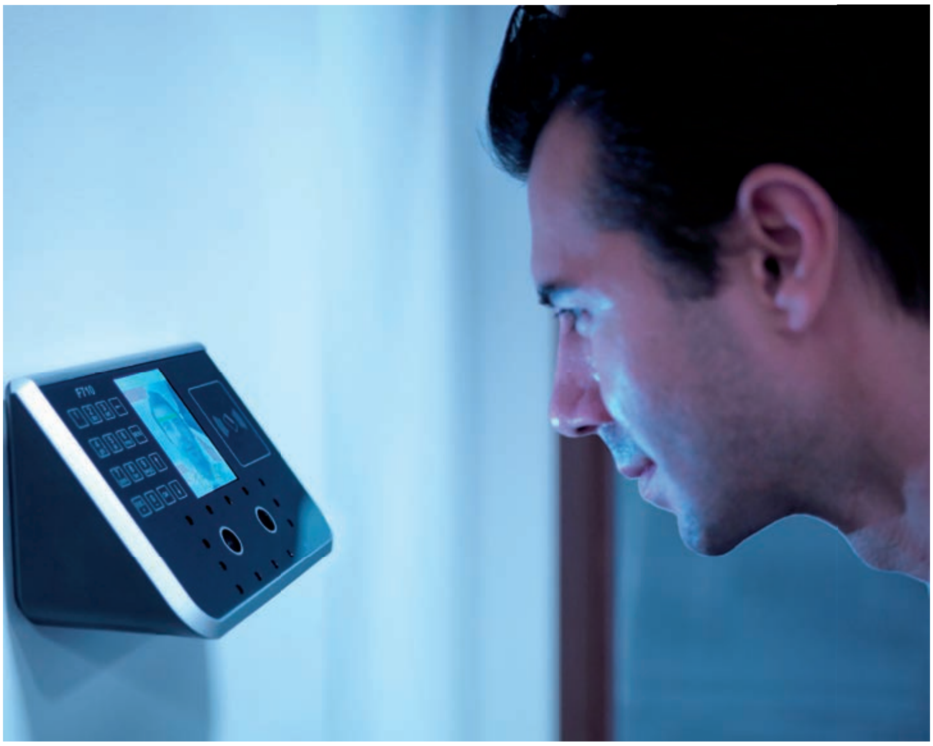
Sharing information

Private sector awareness of the importance of information-sharing has increased in recent years. The Financial Services Information Sharing and Analysis Center (FS-ISAC) is the global financial industry's go-to resource for cyber and physical threat intelligence analysis and sharing. FS-ISAC is unique in that it was created by and for members, and operates as a member-owned non-profit entity.

In many countries, the private sector is working with the public sector to share threat information. Examples include the Cyber Security Information Sharing Partnership in the UK, the European Union Agency for Network and Information Security (ENISA), or Switzerland's Reporting and Analysis Centre for Information Assurance (MELANI).

The CRO Forum has noted a variety of third-party initiatives that have gone live over the last 12 to 18 months, serving as loss database services. For example, DataLossDB8 collects information on data losses as a third party, and is publicly accessible for free. It is an Open Security Foundation project which scans news feeds, blogs and other sources for any data breaches.[38]

[38] CRO Forum, The Cyber Risk Challenge and the Role of Insurance, 2014.



3.3 Actions for policymakers

3.3.1 Strengthening global institutions

Despite the growing perception that cyberspace is unsafe, it would be unwise to call for a complete redesign of the existing regime, as the current system has demonstrated resilience, interconnectivity, and interoperability to a fairly satisfactory degree. Furthermore, an overly-ambitious approach does not seem politically feasible in the current geopolitical environment.

The value of imperfect compromises or suboptimal solutions that will nonetheless allow us to move toward greater cyber security should not be underestimated. Instead of seeking strict international regulation of cyberspace through treaties of doubtful implementation and verification, it will probably prove more effective to focus collective efforts on **strengthening 'fit for purpose' global institutions, whose functions are clear and defined**. G-groupings and INTERPOL, for example, could be crucial for crisis management and for coordinating cross-border law enforcement activities. Due to the deficiencies of the Mutual Legal Assistance Treaty (MLAT) process, it is necessary to increase the degree of harmonization of legislation against cyber crime and create new legal tools to facilitate law-enforcement.

Strengthening such institutions requires a clear understanding of the role each international or regional institution plays. It will be necessary to redefine the mandate of the international institutions that have an impact in cyberspace to avoid overlapping functions, and to increase efficiency. The international community should allocate the global resources of international organizations in the same way as the division of labor; clearly defining and distributing the functions of each.

At the same time, growing political instability could be exploited by authoritarian governments aiming to reduce capabilities and scope of some technical institutions that can provide stability and resilience to cyberspace, thus undermining its multi-stakeholder approach. **Isolating effective cyber governance from the current geopolitical tensions must therefore be a priority**.

> Creating a 'Cyber WHO' could help to address the risk of critical systemic failures."

According to the report 'Beyond Data Breaches: Global Interconnections of Cyber Risk,'[39] the lack of an effective global cyber body could be partially addressed through a **G-20 (states) + 20 (Global Significantly Important Internet Organizations; G-SIIOs) Cyber Stability Board**. Originally informally proposed by Microsoft, a Cyber G20 + 20 would bring together corporate executives who run and maintain the infrastructure, software and protocols of the internet with government leaders. In addition, key governance institutions as ICANN and IETF should also be invited. Analogous to the Financial Stability Board in the financial sector, it could take a leading role in crisis management to deal with cyber shocks and coordinate supporting work to improve risk mitigation and resilience. In this way, the G-20 would have cyber risk management capabilities and the real capacity to deal with systemic failures to prevent a cascade effect.

Informal coordination among central bank governors is one example of a mechanism that proved successful during the financial crisis. This type of coordination was facilitated through personal contacts and networks outside traditional institutions. An informal practice among the various governors has developed that has led them to habitually engage in dialogue, and this has resulted in a better understanding of the impact that individual decisions may have on the whole system. It would be desirable to build similar **informal networks to allow national cyber governance entities to interact**, creating trust, increasing coordination, and facilitating joint responses. To this end, certain steps could be implemented in an incremental way: for example, coordination agreements between law-enforcement agencies (LEAs) and CERTs; early-warning systems; joint cyber security exercises; and adoption of CBMs and risk reduction measures.

The cyber governance landscape is reminiscent of the European integration process: Some states want to move forward with a specific policy while others may oppose it. We therefore believe that the model '**build it and they will come**,' following the example of the European instrument of 'enhanced cooperation,' might be a good idea. Groups of states or enterprises can advance on a specific aspect of global governance by forming a critical mass of players – but always leaving the door open to entry by further nations. In some cases, entry will be driven by economic logic: not joining will become more costly. This would circumvent problems that prevent progress in the governance of cyberspace, such as a lack of trust, insufficient awareness, divergent interests, and institutional inertia.

3.3.2 Managing systemic cyber risks

The ability of the existing global governance regime to deal with crisis management is a field with significant scope for improvement. It would be desirable to have procedures and forums led by international institutions to deal with systemic failures affecting different countries. There should be room for agreement in order to be prepared for a feared 'Cybergeddon'.[40] We therefore propose to use methods in the cyber realm applied to limit the spread of pandemics – after all, infectious diseases and cyber threats not only affect those countries where they have been discovered, and information-sharing is key to stopping dissemination.[41, 42]

Thus the creation of some form of a 'Cyber WHO' should be considered. The World Health Organization (WHO) established the Global Outbreak Alert and Response Network (GOARN) in 2000. GOARN operates as a decentralized network of technical experts, UN regional surveillance programs, and civil society stakeholders. The WHO also established a six-level pandemic alert system based on the geographic spread of the disease and its human transmissibility. Driven by the crises provoked by severe acute respiratory syndrome (SARS) and avian flu (H5N1), WHO member states adopted the International Health Regulations (IHRs) for pandemic preparedness and response. This regulation requires governments to apply measures to increase the quality of incident response in case of a health crisis, communicate health emergencies of international concern to the WHO within 24 hours, and offer immediate access to data. The new IHRs revisions are legally binding – but do not include provisions for enforcement.

[39] Zurich Insurance Group/Atlantic Council. See footnote 1.

[40] Healey, J. (2011) 'The Five Futures of Cyber Conflict and Cooperation,' Atlantic Council. Available at: http://www.atlanticcouncil.org/publications/issue-briefs/the-five-futures-of-cyber-conflict-and-cooperation

[41] Mulvenon, J.C. & Rattray, G.J. (2012) 'Addressing Cyber Instability,' Cyber Conflict Studies Association Rattray, G.J., Evans, C. & Healey, J. (2010) 'American Security in the Cyber Commons' in Contested Commons: The Future of American Power in a Multipolar World, eds. Denmark, A.M. & Mulvenon, J., Center for a New American Security, 137-176. Available at: http://www.cnas.org/files/documents/publications/CNAS%20Contested%20Commons_1.pdf

[42] Rattray, G.J., Evans, C. & Healey, J. (2010) 'American Security in the Cyber Commons' in Contested Commons: The Future of American Power in a Multipolar World, eds. Denmark, A.M. & Mulvenon, J., Center for a New American Security, 137-176. Available at: http://www.cnas.org/files/documents/publications/CNAS%20Contested%20Commons_1.pdf

A Cyber WHO would implement a systemic-failure preparedness system, with a standardized outbreak alert similar to the management of pandemics. Such an alert would trigger specific actions by the local and national cyber authorities nominated to detect and coordinate the response to systemic failures. The system would implement domestic rapid response and information-sharing among interconnected parties, as well as the Cyber WHO and other international cyber authorities. This will require harmonizing current national warning systems and providing incentives to encourage cooperation between governments, businesses and civil society.

Critical information infrastructure protection (CIIP) is another area of systemic cyber risk where there is significant scope for improvement.

Without CIIP, societies cannot function. In many cases, a disruption in one area of critical infrastructure could have a ripple effect that goes beyond the borders of the particular country where the infrastructure is located. Unfortunately, research in protecting these systems has been cut and vulnerabilities have increased since then.[43, 44] ENISA's work in this field is valuable, but global international institutions' involvement in CIIP to address such risks is still patchy and must be improved. Therefore, it is necessary to **stress-test how well prepared critical information infrastructure is for an eventual cyber attack**.

One way to ensure such preparedness would be for an international institution to act as a certifying agent. Such an agent would give scores on cyber security levels. In this way, the institution could verify that it can function in an orderly fashion, and its systems will maintain their integrity in the face of a cyber attack. The institution could also issue cyber security recommendations. A desirable approach would be to use global stress tests to verify the level of cyber security, contingency planning, surveillance, alert systems, and resilience of critical information infrastructures.

Stress test exercises are commonly used to check software and hardware and have also been applied in other fields. The European Central Bank (ECB), in cooperation with the European Banking Authority (EBA), the European Systemic Risk Board (ESRB), the European Commission, and national supervisors, conducted EU-wide stress tests with banks in November 2014 to ensure the stability of the European financial system. In 2011, following the Fukushima nuclear power plant disaster, the European Commission decided to subject all nuclear power plants in the EU to stress tests to ensure that they meet the highest safety standards. Such governance experiences and best practices could be applied to the CIIP field too.

[43] HP (2014) 'Cyber Risk Report 2013'. Available at: http://images.info.arcsight.com/Web/ArcSight/%7B8888e67d-94f4-4904-bb75-35e4dd9f1068%7D_2013_Cyber_Risk(1).pdf

[44] However, some CIIP sectors have attracted the attention of researchers. For example, recently Adam Crain, Chris Sistrunk and Adam Todorsky found more than 25 security vulnerabilities in the communications protocol of the US and Canada power plants and electricity grid.

3.3.3 Enhancing public-private cooperation

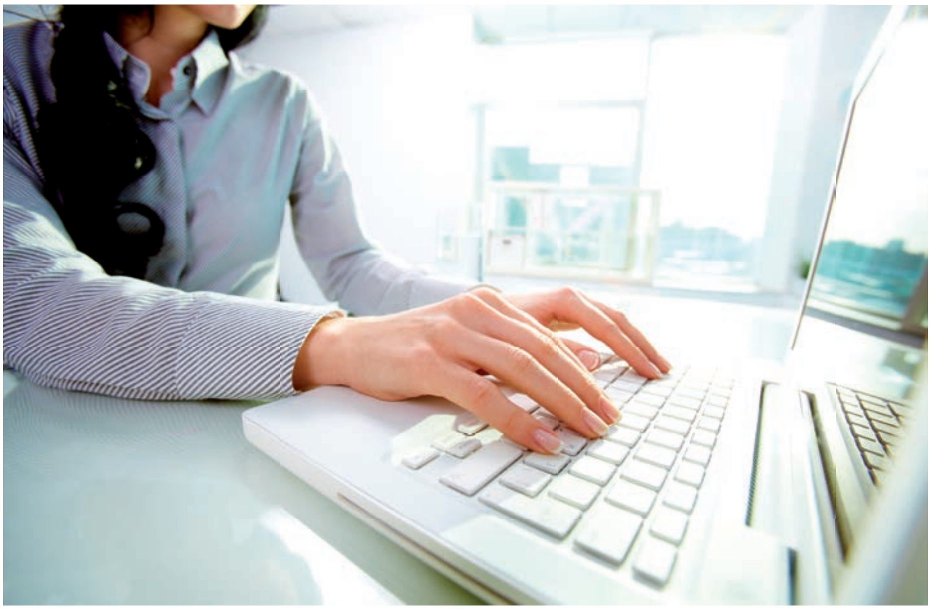
Use incentives to align public- and private-sector interests. Such incentives should encourage the expansion of partnerships and agreements – including between businesses, technical experts, and military, legal, and governmental state authorities. The most effective policies in the cyber domain are those that are shared by both the private and public spheres. Building cooperation schemes is a necessary part of working toward common goals such as developing privacy and data ownership standards. The main areas in which public and private sectors can achieve more synergies are incident response, outreach, information-sharing and policy coordination.

As the private sector becomes increasingly aware of the necessity for cyber security investments, governments and other stakeholders should make an extra effort to **target those public-private organizations that are most effective, especially forums and informal institutions**. Increased transparency over organizational resources and budgets would help to improve this reallocation.

Business should get financial incentives to invest in cyber security. Businesses should get financial incentives to invest in cyber security, for example, third-party audited continuous improvement processes. Industry-driven measures are more likely to create an effective cyber security culture than government-mandated efforts and static lists of security measures. Instilling this culture is a crucial factor in responding collectively to incidents.

As well as providing incentives for public-private cooperation in specialist forums and institutions, the important role of more generalist multi-stakeholder dialogue forums, whose strategic focus includes global governance and cyber risks, should be acknowledged. The World Economic Forum is one such example.

Finally, it will be necessary for the public and private sectors, as well as civil society, to work collaboratively to **ensure that governance in the gray zone is lean, avoids 'gold plating' and has clearly defined objectives**. This will be a challenge given the diverse interests and stakeholders involved.



> Cooperation should be inclusive, and include less-developed countries and civil society organizations."

3.3.4 Increasing inclusiveness

Use private sector globalization as a springboard toward more inclusive cyber governance. The expansion of Asian companies involved in cyberspace is an opportunity to create greater understanding. For example, the Chinese e-commerce company Alibaba's IPO on the New York Stock Exchange was a reminder that its two main shareholders are Yahoo (U.S.) and Softbank (Japan). Similarly, Huawei has a Cyber Security Evaluation Centre (HCSEC) in Banbury, England, which works with the UK intelligence agency GCHQ.

International and regional organizations should pay more attention to the cyber security and critical information infrastructure of LDCs. Strengthening the cyber security capabilities of developing countries through capacity-building, training and technology transfer is key to strengthening the resilience of the entire system.

Lastly, alongside governments and the private sector, **civil society (non-state and not-for-profit organizations) should have a seat at the table when rethinking global cyber governance**. Organizations such as ICT4Peace point out that civil society has an important role to play in promoting inclusiveness, transparency and accountability; deepening knowledge; and fostering trust between states. On the latter point, for example, ICT4Peace is launching a new capacity-building project with different regional organizations. This project is aimed at leveling the playing field, ensuring that all regions are substantively and technically equipped to participate in international and regional ICT-related CBMs and norms processes.[45]

[45] ICTforPeace (2014): 'A Role for Civil Society?'. Geneva 2014.

Conclusion

We are fast approaching a defining moment for global cyber governance. The ubiquity of the internet and impact of emerging technology present huge opportunities for global growth. But at the same time, cyber risks are becoming both more systemic and more interconnected. An effective cyber governance framework is vital if we are to fulfill the promise of the opportunities outlined in this report.

However, such a framework is currently absent. Geopolitical and ideological tensions between states are increasingly being played out in the cyber realm – including over matters of governance. The result has been to limit the coordination and effectiveness of global cyber governance institutions.

Bold recommendations to improve the current situation, such as the creation of a form of Cyber WHO to mitigate against systemic cyber risk, can have a significant impact. But a degree of pragmatism will be just as important. The current geopolitical and ideological tensions are unlikely to be resolved in the next few years, making the consensus needed for whole-scale redesign of the global cyber governance framework a significant challenge. Instead, there should be a focus on strengthening those institutions that work, insulating them from geopolitical tensions and increasing their inclusiveness.

A pragmatic approach will also be important for the private sector. Businesses can be agents of change by championing common values for cyber governance and leading initiatives to close the governance gap. In the meantime, they must respond to the incomplete nature of cyber governance by mitigating against specific cyber risks and increasing their overall cyber resilience.

Governance, no matter how comprehensive, can never nullify all risks. But effective governance can be the key to keeping risks at a manageable level. Given the importance of cyberspace to our world, improving its governance on a global scale is therefore critical.

We hope this report can be of real value to efforts to raise awareness of cyber risks, and realize the benefits that new technologies can provide if these risks are addressed.

Authors: This report is the product of a collaboration between ESADEgeo and Zurich Insurance Group. The project was directed by Angel Pascual-Ramsay at ESADEgeo and Benno Keller at Zurich. The report was researched and written by Angel Pascual-Ramsay, Angel Saz-Carranza and Alvaro Imbernon at ESADEgeo and Benno Keller and David Swaden at Zurich Insurance Group.

Disclaimer

This publication has been prepared by Zurich Insurance Group Ltd and Fundacion ESADE and the opinions expressed therein are those of Zurich Insurance Group Ltd and Fundacion ESADE as of the date of writing and are subject to change without notice.

This publication has been produced solely for informational purposes. The analysis contained and opinions expressed herein are based on numerous assumptions. Different assumptions could result in materially different conclusions. All information contained in this publication have been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Group Ltd or any of its subsidiaries (the 'Zurich Group') or Fundacion ESADE as to their accuracy or completeness.

This publication is not intended to be legal, underwriting, financial, investment or any other type of professional advice. Persons requiring advice should consult an independent adviser. The Zurich Group and Fundacion ESADE disclaim any and all liability whatsoever resulting from the use of or reliance upon this publication. Certain statements in this publication are forward-looking statements, including, but not limited to, statements that are predictions of or indicate future events, trends, plans, developments or objectives. Undue reliance should not be placed on such statements because, by their nature, they are subject to known and unknown risks and uncertainties and can be affected by other factors that could cause actual results, developments and plans and objectives to differ materially from those expressed or implied in the forward-looking statements.

The subject matter of this publication is also not tied to any specific insurance product nor will it ensure coverage under any insurance policy.

This publication may not be reproduced either in whole, or in part, without prior written permission of Zurich Insurance Group Ltd, Mythenquai 2, 8002 Zurich, Switzerland and Fundacion ESADE, Avenida Pedralbes, 60-62, Barcelona, Spain. Zurich Insurance Group Ltd and Fundacion ESADE expressly prohibit the distribution of this publication by or to third parties for any reason. Neither the Zurich Group nor Fundacion ESADE accept liability for any loss arising from the use or distribution of this presentation. This publication is for distribution only under such circumstances as may be permitted by applicable law and regulations. This publication does not constitute an offer or an invitation for the sale or purchase of securities in any jurisdiction.

ESADE
Ramon Llull University
ESADEgeo-CENTER
FOR GLOBAL ECONOMY
AND GEOPOLITICS

Zurich Insurance Company Ltd
Mythenquai 2
8022 Zurich
Switzerland

138488A01 (03/15) ZCA

ZURICH®