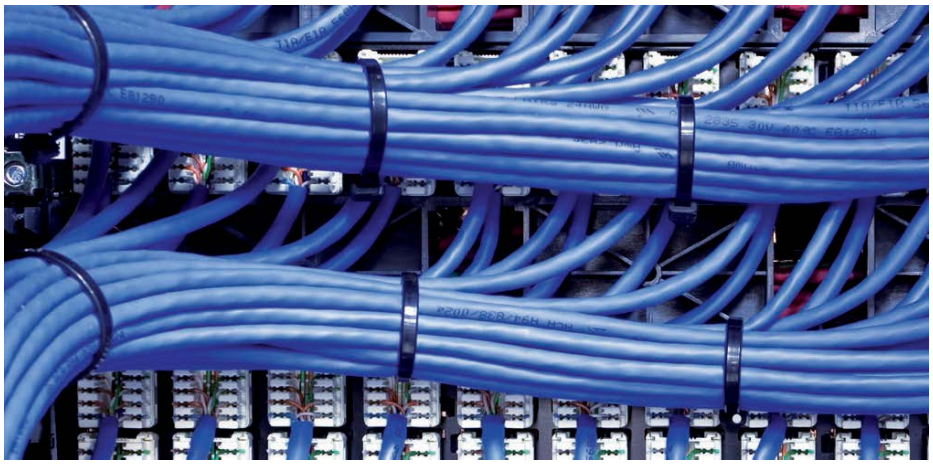
ESADE
Ramon Llull University
ESADEgeo-CENTER
FOR GLOBAL ECONOMY
AND GEOPOLITICS

ZURICH

Risk Nexus

Global cyber governance: executive summary

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.



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

[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

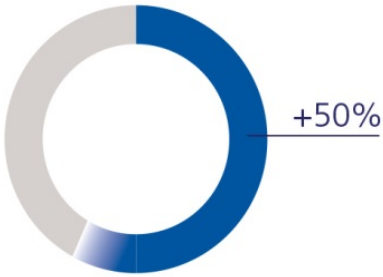
[2] World Economic Forum (2015): 'Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats'. In collaboration with Deloitte, 2015, p.9.

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

Fast fact

Asia leads internet usage

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



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.

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.

The full Risk Nexus report is available on knowledge.zurich.com/cyber-risk/global-cyber-governance/

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.