GCSP
Geneva Centre for Security Policy
Where knowledge meets experience

GCSP Policy Paper 2015/4 - April 2015

Future Challenges in Cyberspace

by Aapo Cederberg

Key Points

- *Cyber power is a global game changer. It brings along new asymmetries to power politics. All aspects of our lives and functions of our societies will be transformed by all-pervasive and hyper connected digitalisation.*
- *The all-pervasive and hyper connected nature of the cyberspace demands that any solutions targeted to increase its security must be comprehensive, taking into account a wide array of sectors and players.*
- *Winners in this new age are those who can combine the comprehensive security solution with a market economy approach, have an ability to amass and mobilise the best talent, and can operate effortlessly in a multi-stakeholder and multinational environment.*

Introduction

Accenture's Technology Vision 2015 report captures well the promise that the still dawning digital age holds for all of us.[1] Connected individuals are able to improve their daily lives by taking advantage of an avalanche of innovative digital services and technologies that have been produced for their use by strongly interconnected companies forming ecosystems. Information flows connect people, companies, societies, and machines, boosting the ability to collaborate, operate more efficiently, and improve the global economy.

While Accenture may have it right, there is also another, more sinister side to technological development, which co-exists with all the promise. The 2015 Global Risks report by the World Economic Forum lists the interlinked technological risks of cyber attacks, critical information infrastructure breakdown, and data fraud or theft as belonging among the top threats to the global economy both now and in near future. Right after the top risks, the report anticipates that the misuse of technology will become a more prevalent threat over the coming decade.[2] Looking from the nation state perspective, the latest U.S. intelligence community's Worldwide Threat Assessment continues to list cyber threats as the number one risk to U.S. security. It would not necessarily be a major source of sudden disruption, but rather an on-going, long-term, low-intensity activity causing cumulative costs, eroding competitiveness, and testing the political resolve and response thresholds.[3]

1 Accenture, *Accenture Technology Vision 2015 - Digital Business Era: Stretch Your Boundaries*, February 2015, http://techtrends.accenture.com/us-en/downloads/Accenture_Technology_Vision_2015.pdf.

2 World Economic Forum, *Global Risks 2015*, 10th Edition, 2015, http://www3.weforum.org/docs/WEF_Global_Risks_2015_Report.pdf.

3 James R. Clapper, "Worldwide Threat Assessment of the US

This policy paper's structure reflects the need for a comprehensive approach to cyber security by offering four different, but complementary perspectives. First of all, the national and international politics are covered, which is followed by a brief look at the interconnected global economy. The third part of the paper discusses security providers, and the final perspective includes civil society and citizens. The paper is concluded with a summary and list of major future trends in cyber security.

Cyber as a Game Changer

The rise of a highly interconnected world, involving all walks of life from international politics and global economics to individual citizens, has already proven to be a strategic game changer. Physical world limitations, including the structures and principles that support it, are still in place. However, the rules of the cyber domain are bending the old barriers of time and space, and changing the structures and the rules of the road. Thus, it can be said that the unfolding world of cyber is very different from the physical world as we know it now.

As always, major changes that can be described as nearly tectonic in their nature, will also give rise to security challenges that players in the security field from individuals to NGOs, to classic security providers such as police and military need to take into account. The unfolding new connections, interdependencies, and ways of operating may bring along many surprises, particularly to those clinging on to the old ways of seeing and doing things.

In addition to the newly shaped operating environment, the idea of cyber power can also be considered a global game changer. It can be argued that cyber brings along new asymmetries to the power politics. The sheer amount of resources and the size of a country or its established political and military alliances may not be the most decisive factor when amassing power and applying force in the cyber domain. It becomes increasingly important to be able to efficiently tap into the national and international knowledge pool and get hold of talented individuals. Highly talented individuals can be considered to be the most dangerous cyber weapon.

The unfolding new connections, interdependencies, and ways of operating may bring along many surprises, particularly to those clinging into the old ways of seeing and doing things.

An ability to amass cyber power and an understanding of how to apply it offers new possibilities to influence politics and security at national, regional and global levels. Cyber power blurs the traditional concepts of military and civilian security as it also blurs the meaning of national borders. The concept of cyber power is challenging the traditional administrative lines within societies by having an impact on all sectors and functions of modern societies. The constant process of developing societies also makes them increasingly dependent on digital structures, and thus on the world of cyber.

National and International Politics

As the discussion above has demonstrated, cyberspace should not be seen only from a technological perspective, but as a phenomenon that has already had, and will continue to have, an ever-greater impact throughout our daily lives and functions of our societies. Thus, cyber aspects should be included in an increased manner both in national and international politics.

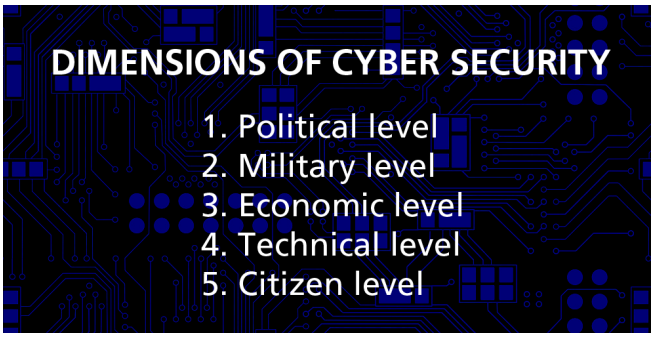
Cyberspace should not be seen only from a technological perspective, but as a phenomena that has already had and will continue to have an ever-greater impact throughout our daily lives and functions of our societies.

National policies are of the utmost importance in building a solid foundation for the establishment of cyber power and constructing more cyber-secure societies. While the national political space for manoeuvring may be limited by international agreements and standards, and most innovation comes from the private sector, national policies still provide the strategic framework for the development of local capabilities. National policies and strategies support intergovernmental collaboration and put in place the educational and industrial policies. National policies are also necessary to support security providers in their work by setting the legal frameworks that define the tools and mandates for security providers. Similarly, national policies define the ways and set the goals for international collaboration.

As the nature of cyberspace is strongly interlinked and international, it is natural that international politics play a major role in defining its functions and uses. While there are various topic areas, where cyber related discussions take place, such as respect for intellectual property rights, innovation and patents; international telecommunications standards; and international laws and norms, what is apparent is that more international, bilateral, and multi-stakeholder collaboration is required.

Intelligence Community" (Office of the Director of National Intelligence, February 26, 2015), http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

All collaboration is based on trust and at the moment it appears that truly global trust in cyber matters is lacking. While this will naturally slow down processes towards achieving truly international consensus on, for example, cyber norms, it should not limit more rapid advances taking place in unofficial or official alliances and bilateral partnerships. The goals for these advances are clear: to increase transparency and build trust among the partners, improve the exchange of information, and to support finding shared goals and agree on common activities towards achieving the goals set.



Interconnected Global Economy

As we have seen with the economic meltdown that began in the United States in 2008 and which is still very much a reality in many European Union countries, the global economy is a highly interconnected network of actors and mechanisms, where a local crisis can turn into a global one.

The global financial networks, which include not only financial institutions, but also secure financial messaging services, such as SWIFT and standards setting organisations like SEPA, are under constant attack, as it was exemplified by attacks against JP Morgan in 2014.[4] The motivations for the attacks vary from criminal intentions to gain financial benefit, to nation states' espionage efforts to better understand the financial structures and money flows between various actors of interest.

While interconnectedness brings new vulnerabilities, the financial networks enable developing economies to effectively and securely support its citizens and countries with monetary flows. According to some sources, these remittances are more than three times larger than global aid budgets.[5] Similarly, modern telecommunications networks and affordable mobile devices provide an efficient platform for micropayment solutions that are very useful in developing economies where many lack access to conventional financial services.[6]

As the financial system and unhindered money flows constitute an important part of the vital functions of both post-industrial and developing economies, it is within the core interests of governments to ensure the functioning of the financial sector and guard it from external attacks. At the same time, while the global financial system can be seen almost as a global common, there needs to be punitive mechanisms such as sanctions that can target the abuse of the cyber side of financial information networks.[7] These mechanisms allow governments working in collaboration with private organisations to weed out actors that are misusing the global system for criminal purposes.

Security Providers – Police & Military

Developments in cyberspace also change the ways in which traditional security providers, e.g. police and military forces conduct their operations. Like citizens and companies, who are more and more integrated into cyberspace, security providers need to establish their presence in the cyber domain to be able to protect individuals, legal entities, and national interests.

Based on news headlines alone, cyber crime is a major headache to police forces around the world. In addition to attacks against financial institutions, cyber criminals extort individual citizens, take over computing resources to sell them as part of botnets, hide their illicit activities in anonymised underground networks, and develop new attack tools both for fellow criminals and for use by their nation state sponsors. Cyber crime is not limited to a certain geographical area, but the crime networks span across the globe, forcing police forces to improve their cross-border activities.

Cyber power blurs the traditional concepts of military and civilian security as it also blurs the meaning of national borders.

While modern police forces are challenged by new types of crime and the transfer of some old forms of crime into cyberspace, there are also developments that support police work both in the physical world and in the cyberspace. Police, like military and the intelligence community, have gained much from the improved ability to process and analyse large

4 Jessica Silver-Greenberg, Matthew Goldstein, and Nicole Perlroth, "JPMorgan Chase Hacking Affects 76 Million Households," *DealBook*, 2 October, 2014, http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/.
5 Claire Provost, "Migrants' Billions Put Aid in the Shade," *The Guardian*, January 30, 2013, http://www.theguardian.com/global-development/2013/jan/30/migrants-billions-overshadow-aid.
6 "Mobile Money in Developing Countries," *The Economist*, 20 September, 2014, http://www.economist.com/news/economic-and-financial-indicators/21618842-mobile-money-developing-countries.
7 Mark Dubowitz and Jonathan Schanzer, "The Fragility of the Global Financial Order," *Wall Street Journal*, 3 March, 2015, sec. Opinion, http://www.wsj.com/articles/mark-dubowitz-and-jonathan-schanzer-the-fragility-of-the-global-financial-order-1425423520.

data sets and produce new insights from it with the help of dedicated software tools. One example of such developments is the concept of predictive policing, where spatially bound crime forecasts can be prepared with the help of software. This enables police departments to apply their scarce resources in a more targeted and efficient manner.[89]

In addition to traditional opponents with their individual capabilities, there are new players in the field that can impact the national security calculus. There is a new set of nations that can develop capabilities to attack their targets across great physical distances through cyberspace, as well as cyber terrorists, cyber militias, and empowered individuals, whose actions can all threaten national security. Regarding potential targets, the most cited example is the vulnerabilities inherent in our critical infrastructure, which could be taken advantage of to create major disruptions that would ripple through society.[10] A similar kind of cascading failure could be envisioned if one of the Internet's key shared computing and storage providers, such as Amazon, were to be taken down.[11]

It can also be argued that the military has been one of the players that has gained the most from the cyber revolution over the past few decades. The early examples include precision-strike capabilities, which combined traditional munitions with information feeds about targets and positions, making the munitions much more efficient in comparison to their traditional counterparts. More recently, advances in communications technologies, robotics, and sensors made it possible to increasingly utilise unmanned platforms both in combat and reconnaissance missions. We have also witnessed cyber weapons that have caused physical damage, like the well-documented case of Stuxnet.[12] The latest example is the heavy-handed information warfare waged by Russia in support of their military intrusion in neighbouring Ukraine. This continued use of information operations can be seen as part of Russia's hybrid warfare doctrine.[13]

8 Joel Rubin, "Stopping Crime before It Starts," *Los Angeles Times*, 21 August, 2010, http://articles.latimes.com/2010/aug/21/local/la-me-predictcrime-20100427-1.
9 Nate Berg, "Predicting Crime, LAPD-Style," *The Guardian*, 25 June, 2014, http://www.theguardian.com/cities/2014/jun/25/predicting-crime-lapd-los-angeles-police-data-analysis-algorithm-minority-report.
10 Richard A Clarke, *Cyber War: The Next Threat to National Security and What to Do About It* (New York, NY: HarperCollins, 2010).
11 Atlantic Council and Zurich Insurance Company, *Beyond Data Breaches: Global Interconnections of Cyber Risk*, Risk Nexus, April 2014, http://www.atlanticcouncil.org/images/publications/Zurich_Cyber_Risk_April_2014.pdf.
12 Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *WIRED*, 11 March, 2014, http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
13 Janis Berzinš, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy,* Policy Paper (Center for Security and Strategic Research, National Defence Academy of Latvia, April 2014), http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx.

Civil Society and Citizens

All the way from the invention of the printing press, and particularly since the early industrial age, we have witnessed relatively rapid change where technology and culture have been in constant interplay. Culture has had an impact on the ways new technological advances have unfolded and, similarly, technology has changed the ways that citizens live their daily lives and utilise the resources at their disposal. Therefore, technology can be a driver for change. Nevertheless, the changes are rarely neutral. Sometimes, technological advancements outpace stagnated societies and norms, which may lead into friction and, in the worst cases, conflict.

According to some statements, social media tools constituted one of the catalysts that set off the events that have taken place in the Arab world since 2011.[14] While the so called Arab Spring and its aftermath is one of the most cited examples of technology infused activism, cyber activism in its various forms is taking place on a daily basis at the global level. Because of this, some countries see technologies that enable freedom of speech and support the organisation of civil society as a threat to their undemocratic ways of governing and thus something that needs to be carefully controlled.[15] Technologies that can be used for benevolent purposes, such as to inform and liberate, can also be used for malevolent purposes, such as to stifle, intimidate, and misinform.

Finding the right balance between individuals' rights and the nation states' responsibility to protect their societies and citizens is one of key topics defining the on-going cyber security narrative.

An important aspect of cyber security from an individual citizens' perspective is unobstructed access to information, the ability to speak out and contribute by utilising local and global information platforms, permission to reach out to other people and organisations around the world, and a reasonable expectation of privacy and information security. From the open society's perspective, it is the society's responsibility to provide its citizens and other legal entities with unbiased information, to allow access and ability to contribute to global information flows, and to ensure the security of information networks. It is also within society's responsibilities to shield citizens in various ways from

14 Philip N. Howard et al., *Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?*, Working Paper, Project on Information Technology and Political Islam, (September 2011), http://pitpi.org/wp-content/uploads/2013/02/2011_Howard-Duffy-Freelon-Hussain-Mari-Mazaid_pITPI.pdf.
15 Beina Xu, "Media Censorship in China," *Council on Foreign Relations*, 25 September, 2014, http://www.cfr.org/china/media-censorship-china/p11515.

malicious actors, whether they are criminal hackers trying to penetrate devices, or nation states sending out propaganda to confuse the minds of the citizens. Finding the right balance between individuals' rights and the nation states' responsibility to protect their societies and citizens is one of key topics defining the on-going cyber security narrative.

Conclusions

The discussion that took place earlier in this paper was intended to show the all-pervasiveness of cyber elements throughout our societies and their functions. It can be argued that it is impossible to have a modern, well functioning society without having a reliable and robust system in place to ensure the security of the cyber domain. Cyberspace is at the same time a great opportunity and promise, but also a risk that must be properly managed.

Countries and other actors see cyberspace in very different lights. For some, it is a business opportunity, or a medium for self-expression, while others see it as a threat to national security. While there are numerous examples of technology used for malevolent purposes, our experience also tells us that affordable access to communications technologies and global information flows can be a force for democratising movements across the globe.

All the above emphasises the multidimensionality of cyber security. While the cyber revolution has already been on-going for a few decades, we have just seen the dawn of the cyberspace as a global game changer and thus it is not easy to accurately predict its future development.

However, there are some major trends can be spotted already at this point:

1. Digitalisation will continue and it will penetrate all aspects of our lives and functions of our societies.
2. People will become more and more dependent on digital services and various kinds of information and communications technologies, which will support the public interest in cyber security both by citizens and media.
3. Modern societies will become more and more vulnerable in the future as the complex interconnected and interdependent systems are difficult to fully comprehend and protect.
4. Global interdependencies will increase together with intra-societal dependencies, making the cyber security challenges increasingly global in nature. Thus there is a need for international responses to the threats that we face as they continue to grow.
5. The number of new technological innovations coming mostly from private sector players will increase and in terms of security, the consequences will continue to be two-fold – there are aspects to the new innovations that both enhance and threaten security.
6. There will also be a number of novel technologies that will provide us with better and more sophisticated solutions for cyber security. Nevertheless, the cyber arms race will continue in a manner analogous to the tank-antitank weapons development race.
7. Cyber crime will continue to challenge societies and the economic losses because of it will grow. On the other hand, this development will facilitate collaboration between the public and private sectors.
8. The concept of cyber power will have an impact on international politics and the global struggle for power. This will also support the trend leading us to a growing arms race in the cyber domain.
9. It is highly likely that there will be a global cyber catastrophe in the near future, which will change our attitudes towards cyber security in general and towards international collaboration needed to secure the cyberspace.
10. Lastly, the winners in the cyber domain are those who are able to balance the security needs and economic potential in cyberspace. The balancing act demands a comprehensive approach instead of a militarised solution, and it will need to mobilise resources from all parts of society to solve the common challenge.

About the author:

Aapo Cederberg is a retired colonel from the Finnish Armed Forces and is Senior Programme Advisor in the Emerging Security Challenges Programme at GCSP. He was previously the Secretary General for the Finnish Security Committee and prior to that was the Head of Strategic Planning in the Ministry of Defence.

NB: This paper is solely the opinion of the author and does not necessarily reflect the official view of the GCSP.

All GCSP Policy Papers are available at www.gcsp.ch.