Research Series

7 - 2012 GenevaPapers

Meeting the Cyber Security Challenge

Gustav Lindstrom

GCSP

The opinions and views expressed in this document do not necessarily reflect the position of the Swiss authorities or the Geneva Centre for Security Policy.

Copyright © Geneva Centre for Security Policy, 2012

100%
FSC
www.fsc.org
RECYCLÉ
Papier fait à partir
de matériaux recyclés
FSC® C103623

Meeting the Cyber Security Challenge

Gustav Lindstrom

GCSP Geneva Papers — Research Series n° 7, June 2012

The Geneva Centre for Security Policy

The Geneva Centre for Security Policy (GCSP) is an international training centre for security policy based in Geneva. An international foundation with over forty member states, it offers courses for civil servants, diplomats and military officers from all over the world. Through research, workshops and conferences it provides an internationally recognized forum for dialogue on timely issues relating to security and peace.

The Geneva Papers and l'Esprit de Genève

With its vocation for peace, Geneva is the city where international organizations, NGOs, and the academic community, working together, have the possibility of creating the essential conditions for debate and concrete action. The *Geneva Papers* intend to serve the same goal by promoting a platform for constructive and substantive dialogue.

Geneva Papers – Research Series

The *Geneva Papers – Research Series* is a new set of publications offered by the GCSP. It complements the *Geneva Papers – Conference Series* that was launched in 2008, whose purpose is to reflect on the main issues and debates of an event organized by the GCSP.

The *Geneva Papers – Research Series* seeks to analyse international security issues through an approach that combines policy analysis and academic rigor. It encourages reflection on new and traditional security issues that are relevant to GCSP training, such as the globalization of security, new threats to international security, conflict trends and conflict management, transatlantic and European security, the role of international institutions in security governance, and human security.

The *Research Series* offers innovative analyses, case studies, policy prescriptions, and critiques, to encourage discussion in International Geneva and beyond.

Drafts are peer-reviewed by the GCSP Review Committee.
All *Geneva Papers* are available online, at www.gcsp.ch/Resources-Publications/Publications

For further information, please contact :
Anne-Caroline Pissis, External Relations Manager : a.pissis@gcsp.ch

Series Editor : Thierry Tardy

Copyright © Geneva Centre for Security Policy, 2012

Table of Contents

About the Author

Dr Gustav Lindstrom is Head of the Euro-Atlantic Security Programme and Course Director of the European Training Course in Security Policy (ETC) at the Geneva Centre for Security Policy (GCSP). He received his doctorate in Policy Analysis from the RAND Graduate School and M.A. in International Policy Studies from Stanford University. Prior to his tenure at the GCSP, Dr Lindstrom served as a Senior Research Fellow at the EU Institute for Security Studies (EUISS) in Paris. His areas of expertise include transatlantic relations, the EU's Common Security and Defence Policy (CSDP), terrorism, non-proliferation, and cyber security.

List of Acronyms

ATM	Automated Teller Machine
CERT	Computer Emergency Response Team
CoE	Council of Europe
CSIRT	Computer Security Incident Response Team
CSIS	Center for Strategic and International Studies
DARPA	Defense Advanced Research Projects Agency
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DNSSEC	Domain Name System Security Extensions
EMP	Electromagnetic Pulse
ENISA	European Network and Information Security Agency
EU	European Union
GGE	Group of Governmental Experts
GSM	*Groupe Spécial Mobile* (Global System for Mobile Communications)
ICANN	International Corporation for Assigned Names and Numbers
ICS	Industrial Control System
IHL	International Humanitarian Law
IPv6	Internet Protocol Version 6
IT	Information Technology
ITU	International Telecommunication Union
LoAC	Law of Armed Conflict
NATO	North Atlantic Treaty Organization
OECD	Organization for Economic Cooperation and Development
Malware	Malicious Software
RFID	Radio Frequency Identification Device
SCADA	Supervisory Control and Data Acquisition System
SIM	Subscriber Identity Module

Executive Summary

While most policymakers agree that there are substantial risks in cyber space, there is disagreement on whether or not it poses a threat to national security. The divergence in opinions is most obvious when references are made to terms such as cyber war and cyber warfare. In spite of these differences, there are many reasons why policymakers should care about developments in cyber space. With society's growing reliance on cyber space, a disruption can have wide ranging implications and cascading effects.

At the level of national security, there are also indications that government systems are routinely probed for weaknesses. It comes as no surprise that the losses from sabotage, the theft of intellectual property, and cyber crime are counted in the billions of Euros. While the prospects of cyber war are unlikely, it is increasingly evident that a cyber dimension is likely to be part of future conflicts. According to a preliminary assessment carried out by the Center for Strategic and International Studies (CSIS) in Washington, DC, 33 countries presently include cyber warfare in their military planning and organization. These might include "cyber capabilities for reconnaissance, information operations, the disruption of critical networks, for 'cyber-attacks', and as a complement to electronic warfare and information operations."[1]

In response, there are a number of measures being undertaken to address different types of cyber security challenges. These include both technical and institutional means that can be applied in a preventive and consequence management situation. Key among these measures are raising awareness of cyber risks and promoting international cooperation. Looking ahead, policymakers in national security will have to give careful consideration to three key issues:

[1] J. Lewis and K. Timlin, "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization", Center for Strategic and International Studies, Washington, DC, 2011, p.3. Accessed on 7/05/2012 at http://www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf

- *Finding a balance between defensive and offensive cyber capabilities* – What are the implications of a shift to more offensive cyber capabilities? For example, could it lead to a cyber arms race? How might it affect the future conduct of warfare?

- *Clarifying the legal landscape and the application of international law* – A key question is whether a cyber operation can be equated to an armed attack or a wrongful threat or use of force.

- *Examining the prospects for or against an Internet governance model* – Specifically, is there need for a more formal government role to manage the Internet?

Regardless of the paths taken, the choices will have longstanding implications for cyber security and how cyber space is used in the future.

Introduction[2]

The link between cyber security and national security is a recent phenomenon.[3] As of 2000, an increasing number of national security strategies and white papers link cyber security to one of three aspects associated with national security: the need to protect critical infrastructures, the need to ensure economic security (e.g. limiting the loss of intellectual property), and the need to gauge the implications of new technologies on the conduct of warfare.[4] To illustrate, the national security strategies of Hungary (2004), the Czech Republic (2008), Finland (2009), Switzerland (2009), the United States (2010), the United Kingdom (2010), and Austria (2011) make reference to at least one of these three dimensions.

Another trend that points to a growing link between cyber security and national security is the establishment of specific cyber security strategies at the national level. In 2011 alone, at least eight countries unveiled such strategies: Colombia, France, Germany, India, the Netherlands, New Zealand, the United Kingdom (its second), and the United States.

While cyber security is increasingly on the agenda of policymakers, there is no commonly held view on the scope of the cyber threat or how to best address it. The range of opinions go from those who believe that government officials are being too slow to recognise the scale of cyber challenges to those who view cyber challenges more as a nuisance than as a security threat.

[2] A note of gratitude is extended to Thierry Tardy for his thoughtful review and comments on this paper as well as to Charles Simpson for his editorial support.

[3] According to the International Telecommunication Union, cyber security is "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment." See http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[4] Although this paper does not focus on the numerous positive implications of cyber space, it should be acknowledged that many strategies include a cyber dimension given its perception as a vehicle for economic growth and innovation.

With this in mind, this research paper examines some of the principal cyber security challenges and the measures taken at the national and international level to respond to them. It is organized as follows. Chapter 1 examines reasons why the policy community should care about cyber security. Chapter 2 then identifies the principal cyber security challenges – those primarily targeted at individual users and those affecting national security – and their implications. Chapter 3 highlights some of the main preventive and consequence-management measures available to mitigate the effects of cyber threats. Chapter 4 highlights cyber issues for future consideration. Annex A offers a glossary of the technical terms used in the paper.

This research paper is targeted to officials and academics interested in broadening their understanding of cyber security, its related challenges, and the measures available to address them.[5] In particular, it may be of interest to individuals working in the field on national security. To the extent possible, the paper avoids delving into the technical dimensions of cyber security and focuses on the policy domain level.

[5] It should be noted that this paper does not delve into the extensive benefit accruing to society from access to cyber space and its applications.

Why Should We Care About Cyber Security?

From a policy perspective, there are at least five reasons why policymakers should care about cyber security. First, there is a growing number of individuals who use the Internet, and many of these new users are unfamiliar with risks in cyberspace.[6] To illustrate, the number of Internet users around the world in 2000 was approximately 361 million; at the end of 2011, the figure had grown to 2.27 billion – more than a six-fold increase in a little over ten years.[7] The individuals who have entered cyberspace over the last decade are experiencing a much more sophisticated Internet. For example, those who are not aware of how to protect their computers are more likely to be prey for advanced malicious software (malware) that was nonexistent a decade ago. As shown in Table 1, the vast majority of new users are from the developing world where cyber security culture is still in its infancy and protective systems may be out of reach to many users – either due to financial constraints or availability.

Table 1: Internet Users by Region for 2000 and 2011

Region	Internet Users in Dec. 2000 (in millions)	Internet Users in Dec. 2011 (in millions)	Growth 2000-2011 (in percent)
Africa	4.5	139.9	2,988
Asia	114.3	1,016.8	790
Europe	105.1	500.7	376
Middle East	3.3	77.0	2,245
North America	108.1	273.1	153
Latin America / Caribbean	18.1	235.8	1,205
Oceania / Australia	7.6	24.0	214

Source: http://www.internetworldstats.com/stats.htm

[6] Cyber space here is understood as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries". This definition stems from National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23), 8 January 2008.

[7] Data accessed on 16/04/2012 at http://www.internetworldstats.com/stats.htm

Second, the number of cyber-related applications has increased steadily over the past two decades. When the Internet was first developed by the Defense Advanced Research Projects Agency (DARPA) in the late 1960s, its developers could not have fathomed the number of video, voice, and e-service applications that would be spawned in the future. As more individuals rely on services such as e-commerce and e-banking, the greater the risks to society should a service be compromised. A greater reliance on Internet-based services also attracts criminal groups which seek new avenues to make money. Criminal groups are continually exploring new ways to hack into technologies such as credit cards, automated teller machines (ATMs), and Radio Frequency Identification Devices (RFID). According to the 2011 Norton Cybercrime Report, the yearly global cost of cyber crime is about USD 388 billion, approaching the value of all global drug trafficking estimated at USD 411 billion.[8] These vulnerabilities extend to new technologies such as smart mobile phones, compounding the ways in which individuals can be targeted. For example in September 2010, a virus was able to infect over a million smart phones in China – accessing the phone's SIM (Subscriber Identity Module) Card and sending spam text messages to all contacts listed in the address book.[9]

Third, critical infrastructures are becoming more vulnerable to cyber attacks. The Achilles heel of these infrastructures is their industrial control systems (ICS) such as supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS). ICS were initially designed with proprietary technology and were separate from other existing corporate networks, such as local area networks and wide area networks.[10] Because of this separate architecture, the systems were not prone to external electronic attacks. Over time, the drive for cost efficiency and the availability of commercial off-the-shelf technology led to a greater reliance on widely distributed operating systems such as Windows to enhance time-critical response and competitiveness. As a result, many of today's ICS are connected to the Internet and can be accessed remotely.

Connecting industrial control systems to the Internet has important implications. It exposes the control systems to hacking, worms, viruses, and a number of other vulnerabilities that can be introduced through the Internet, intranets,

[8] 2011 Norton Cyber Cybercrime Report, J. Labrie *et al.*, accessed on 16/05/2012 at http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/#nav

[9] S. Kolesnikov-Jessop, "Hackers Go After the Smartphone", *The New York Times*, 13 February 2011.

[10] The two principal categories of industrial control systems are distributed control systems (often found in power plants, refineries, and chemical plants) and supervisory control and data acquisition which are usually employed for distribution operations for water systems, electrical lines, and gas pipelines.

remote dial-up, and wireless applications.[11] The vulnerability is compounded by merging common information technologies such as Ethernets, Windows, and Web Services into ICS.[12] With access to an ICS, an outsider may be able to affect physical processes such as the temperature, flow rate, or rotation speed within a critical infrastructure. Other potential actions include the ability to set thresholds for preventing shutdowns, and opening or closing circuit breakers. In July 2010, US authorities discovered malicious software that was specifically authored to attack the industrial control systems frequently used in electric power plants.[13] In 2010, the targeting of Iran's nuclear facilities via the Stuxnet virus demonstrated how a specific ICS could be sabotaged remotely.

As many critical infrastructures depend on the electricity grid for their operation, there is also a risk of "cascading effects" should a particularly sensitive infrastructure be compromised. It is also possible that an impact on the electricity grid – such as a line outage or system condition problems – could impact grid reliability in other regions given the high interdependence across the components of the electricity grid.[14]

Fourth, malicious cyber activities are becoming more sophisticated and easier to execute. Individuals interested in mounting a cyber attack do not need to have any advanced knowledge of computer programming, as they can purchase off-the-shelf crime kit tool ware. An example of such programmes is the Zeus crime kit whose malicious code can be customized. Several thousand variants of Zeus exist, the average asking price ranging in the neighbourhood of USD 700.[15] Some versions of the source code for this banking Trojan horse is available on the Internet.[16] As shown in Table 2, a menu of different fraudulent services is available for sale, spanning stolen credit card numbers to access to compromised computers (also known as botnets).

[11] T. Datz, "Out of Control", cso-online, 1 August 2004, accessed on 12/11/2011 at http://www.cio.com/article/219486/SCADA_System_Security_Out_of_Control.

[12] E. Byres and J. Lowe, "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems", British Columbia Institute of Technology (BCIT) and PA Consulting Group, October 2004.

[13] See "Grid Cyber Security Act", 112 Congress, 1st Session, Senate Report 112-34, 11 July 2011.

[14] *Ibid*.

[15] D. Macdonald, "Zeus: God of DIY Botnet", Fortinet, accessed on 14/05/2012 at http://www.fortiguard.com/analysis/zeusanalysis.html

[16] P. Kruse, "Complete ZeuS Sourcecode Has Been Leaked to the Masses", Blog entry, CSIS Security Group, Copenhagen, May 2011, accessed on 8/05/2012 at http://www.csis.dk/en/csis/blog/3229/

Table 2: Sample of Illegal Services for Sale and Indicative Price Range (2010)

Item	Bundle Size	Price (in USD)
Access to botnets	10,000	15
Provision of stolen credit card information	10 credit cards	1.70
	100 credit cards	1.00
	750 credit cards	0.70
	1,000 credit cards	0.30
Access to credit card dumps	101 dumps	0.50
Access to stolen identities (full)	30 full identities	0.67
	100 full identities	0.50

Sources: Goods and services available for sale on underground economy servers, 2010, Symantec Corporation. http://www.symantec.com/threatreport/topic.jsp?id=fraud_activity_trends&aid=underground_economy_servers; Symantec Internet Security Threat Report, Vol. 16, April 2011, available at http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=threat_report_16

Fifth, there is a wide range of individuals and groups who may be interested in using cyber space for questionable objectives. While there is a tendency to focus on specific groups such as organized crime seeking financial gain and terrorists who might utilize the web to communicate and spread their ideologies, there are other profiles of individuals who could threaten cyber security. These include organizations and groups interested in accessing sensitive information from government sources or international organizations. International organizations such as the European Union (EU) and the Organization for Economic Cooperation and Development (OECD) have been targeted in the past. In the case of the OECD, hackers were able to gain access to sensitive information on money laundering, high-level corruption, and tax evasion.[17]

As shown in Table 3, there are numerous categories of individuals and groups who could threaten cyber space. These include script kiddies, hacktivists, and botnet operators. Complicating the threat picture are the groups' different motivations and methodologies to reach their ends. With these elements in mind, the next section examines some of the principal cyber security challenges.

[17] A. Rettman, "Hackers Break into OECD Computer System", *EUobserver*, 4 November 2010.

Table 3: Actors Who May Threaten Cyber Security, Motivation, and Types of Attack

Group	Motivation	Type of Attack
Script kiddies	Curiosity / Reputation	Readily available software
Hackers	Challenge of breaking new defences Financial gain	Use of automated tools; potential for co-ordinated attacks
Insiders	Revenge / extortion	Multiple possibilities
Hacktivists	Propaganda (political, social, economic, religious)	Same as script kiddies / hackers
Criminal groups	Financial gain	Phishing, pharming, spam
Spyware/malware authors	Mainly financial gain	Same as criminal groups
Botnet operators	Financial gain / cause disruption	Use of remotely controlled systems
Terrorists	Propaganda (political, social, economic, religious) Cause disruption / damage	Multiple possibilities, includingattacks on critical infrastructures
States	Cause disruption / damage Espionage / gather intelligence	Multiple possibilities

Sources: S. Baldi, E. Gelbstein, and J. Kurbalija, *Hacktivism, Cyber-Terrorism, and Cyberwar*, The Information Society Library, DiploFoundation, Geneva, Switzerland, 2003 and US Government Accountability Office (GAO) Report "Cyberspace", Washington, DC, GAO-10-606, July 2010.

What Are the Principal Cyber Security Challenges?

Cyber security challenges can take many forms, although most are targeted to individuals or organizations. Depending on the nature and method of attack, a cyber operation may also have an impact at the national level. The following section outlines some of the principal cyber security challenges, covering first those that tend to affect individual users and then examining those which may have implications at the national or international level.

Cyber security challenges primarily impacting the individual user

Cyber security challenges that target individuals or organizations may result in the loss of sensitive information, lead to financial loss, facilitate repeat attacks (including on critical infrastructures), or facilitate a distributed denial of service (DDoS) attack. At least three cyber security challenges may affect individual users.

First, many users are unaware of how their computers could be compromised by malicious software (malware). They may not even be aware that their computers or other affected systems could be used without their knowledge. On any given day, thousands of computers fall prey to a variety of computer viruses, worms, Trojan horses, or blended threats which combine aspects of different malware. Advances in programming to evade detection, known as rootkits, also serve to mask these new types of malware.[18] While many individual users fall prey to rudimentary malware that results in limited effects – e.g. a slower computer or the deletion of certain files – many may have their identities stolen or have their computer inadvertently take part in a DDoS attack. According to Norton's 2011 Internet Security Threat Report, Symantec encountered over 286 million unique variants of malware in 2010.[19]

Existing technologies can also be combined in novel ways to either protect or compromise data. A recent example unveiled at the conference for security professionals held yearly in Las Vegas (known as Black Hat) was the "Wireless

[18] For example, rootkits of concern include Tidserv, Mebratix, and Mebroot.

[19] Symantec Internet Security Threat Report, Vol.17, April 2012, Mountain View, California, available at http://www.symantec.com/threatreport/

Aerial Surveillance Platform". It represents a homemade drone that can tap into wireless networks from the air. The platform can also feign to be a Global System for Mobile Communications (GSM) cell phone tower, enabling it to listen in on calls and text messages that go through it. Built at a cost of about USD 6,000 with commercial off-the-shelf materials, it is likely to attract the attention of individuals, organizations, and even countries who may want a cheap means to eavesdrop on specific communications.[20] Further ahead, technologies now slowly entering the marketplace – such as 3-dimensional printing – could also increase security risks in some areas although they typically bring about substantially more positive than negative effects.[21]

Attack techniques are also evolving, exacerbating the risks to users who may be unaware of danger signs. For example, many users may fall prey to "phishing" attacks, in which recipients of fraudulent e-mails or instant messages are asked to provide sensitive personal information such as credit card details, usernames or passwords. In 2011, there were about 200,000 unique phishing attacks worldwide.[22] Among the most common phishing targets are companies such as PayPal and Taobao.com (a Chinese e-commerce site). Targeted attacks on specific individuals, commonly known as "spear phishing", is now possible as attackers use information gleaned from victims' social media activity, making it more difficult to discover an attack.

Even "benign" techniques, mainly intended to display dissatisfaction can have unintended consequences. To illustrate, in August 2011, an individual used his twitter account to incite his nearly 600,000 followers to take part in a telephone blitz against the Los Angeles County sheriff's department – one of the busiest stations in the country. Callers were instructed to contact the station and ask for an internship. As a result, the station's emergency phone system was overwhelmed.[23]

A second cyber security challenge is the slow pace of national and international legislation to tackle malicious online activity and new forms of cyber crime. Lack of progress in this area enables attackers to exploit loopholes and develop

[20] See S. Sengupta, "A Homemade Drone Snoops on Wireless Networks", *The New York Times*, 5 August 2011.

[21] For examples of possible risks associated with 3-D printing, see D. Draeger, "3-D Printing's Radical New World", Salon.com, accessed on 23/05/2012 at http://www.salon.com/2012/05/16/3_d_printings_radical_new_world/singleton/

[22] G. Aron and R. Rasmussen, "Global Phishing Survey: Trends and Domain Name Use in 2H2011", APWG, Lexington, Massachusetts, April 2012, accessed on 18/05/2012 at http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2011.pdf

[23] "Tweeting Rapper May Face Charges", *The International Herald Tribune*, 15 August 2011, p.7.

new means to target users. For example, limited harmonisation in international laws against cyber crime and other online activities – such as sending spam – allow individuals or groups to transfer their activities to countries were national legislation against specific malicious activity is either weak or altogether missing. As shown in Table 4, different countries top the list depending on the malicious activity monitored. For example in the case of Brazil, which often ranks first in the area of spam, there is no specific law to deal with spam.

Table 4: Malicious Activity by Country of Origin (2009)

Overall Rank 2009	Country	Malicious Code (Rank)	Spam (Rank)	Phishing Hosts (Rank)	Bots (Rank)
1	United States	1	6	1	1
2	China	3	8	6	2
3	Brazil	5	1	12	3
4	Germany	21	7	2	5
5	India	2	3	21	20
6	United Kingdom	4	19	7	14
7	Russia	12	2	5	19
8	Poland	23	4	8	8
9	Italy	16	9	18	6
10	Spain	14	11	11	7

Source: Symantec Global Internet Security Threat Report, April 2010.

Diverging national policies is reflected in the low adhesion numbers to the Council of Europe (CoE) Convention on Cybercrime. Opened for signature in late 2001 and entering into force in 2004, it has only 33 State Parties as of mid 2012.[24] An additional 14 countries have signed but not ratified the Convention.[25] Also known as the Budapest Convention, the treaty serves as a guideline for countries developing national legislation against cyber crime and as a framework for harmonizing national laws.

With legal instruments evolving slowly, they may also fail to take into account new developments in cyber space. For example within the EU, a draft law developed by the European Commission in 2010 to make it a crime to launch a malware attack on government or private company servers is still [as of October

[24] For more information on this Convention, see http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG

[25] Data as of May 2012, accessed on 15/05/2012 at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

2011] in the early stages of parliamentary work. Given the delays, some argue the effort is already out of date as it does not consider issues such as "jurisdiction over social networks [...] or security breaches in cloud data centres".[26]

A third challenge, which is not too prominent today, is ensuring continuity of service / access to the Internet. This challenge is likely to increase as societal dependence on cyber space grows. One dimension is the need to protect the physical backbone of the Internet. While the Internet was constructed to be robust, it has certain weaknesses. An example is the principal submarine cables that connect different countries and regions to the Internet. More than ninety percent of Internet traffic is carried via undersea fibre optic cables. There have been several cases of damaged or stolen cables which have impacted services to millions of users for time spans ranging from a few hours to several days. The disruptions to these undersea cables can take many different forms, for example:[27]

- in July 2005, a portion of the SEA-ME-WE[28] 3 submarine cable, which is among the longest in the world, was disrupted so the majority of Pakistani voice and data communications were disrupted for several hours;[29]
- in 2007, pirates stole 11 kilometres of the T-V-H[30] submarine cable, affecting millions of Internet users in Vietnam. Several optimal amplifiers were out of commission for approximately 80 days until replacements could be inserted;[31]
- in 2011, most of Armenia lost access to the Internet for roughly five hours when an elderly woman looking for copper in neighbouring Georgia accidentally damaged a fibre optic link while digging with a shovel. Substantial portions of Georgia and Azerbaijan were likewise affected.[32]

When several of these cables are in close geographic proximity they constitute a sensitive chokepoint. Chokepoints can be found around New York, the Red Sea, and the Luzon Strait in the Philippines.[33] Should these be targeted or vandalized, the implications to society could be much greater than the examples provided above.

[26] V. Pop, "EU Struggling to Fight Cyber Crime", *EUobserver*, 11 October 2011.

[27] B. Daviss, "Building a Crash-Proof Internet", *New Scientist*, No. 2714, 29 June 2009.

[28] South East Asia-Middle East-Western Europe.

[29] See "Submarine Cables and the Oceans: Connecting the World", International Cable Protection Committee, Cambridge, United Kingdom, 2009, accessed on 15/12/2012 at http://www.iscpc.org/publications/ICPC-UNEP_Report.pdf

[30] Thailand-Vietnam-Hong Kong.

[31] D. Burnett, "Cable Vision", *Proceedings,* US Naval Institute, Annapolis, Maryland, August 2011.

[32] T. Parfitt, "Georgian Woman Cuts Off Web Access to Whole of Armenia", *The Guardian*, 6 April 2011.

[33] See "War in the Fifth Domain", Briefing Cyberwar, *The Economist*, 3 July 2010.

Beyond stolen or damaged hardware, countries themselves can affect Internet access. As was demonstrated during the Arab spring uprising in Egypt in 2011, officials were able to shut off Internet access to the population overnight. On 28 January 2011, Egypt went "offline" for approximately five days, demonstrating the ability to effectively shut off the access for a country. While such a move is a national prerogative imposed by government officials, the impacts may be felt in neighbouring countries as business links and communications across borders are affected.

Cyber security challenges primarily impacting national security

Several cyber security challenges may impact national security.[34] First, and as noted earlier, malware that primarily impact individual users or organizations may spill-over and have effects at the national level – especially when a large number of individuals are affected. To illustrate, the Conficker worm, which was first identified in November 2008 and has infected over 12 million computer users to date, also had a national security impact in several countries. In France, the French Navy had to ground several aircraft as flight plans could not be downloaded into the cockpit system. In Germany, several computers belonging to the Bundeswehr were infected and thus out of commission.[35] Another example is the W32.Blaster Worm which in August 2003 aggravated the blackout that hit the East coast of the United States. While it had no direct impact on national security, the blackout affected several million people and its economic costs ranged from USD 7 to 10 billion.[36]

Second, some countries may fall victim to a DDoS attack like the one that hit Estonia in April-May 2007. The possible ramifications of such attacks are wide ranging. In the case of Estonia, a country whose population is highly Information Technology (IT)-dependent, the effects were felt extensively as e-banking, e-government services, communications systems, and media went offline or was severely impacted. Websites that on average received around 1,000 visits per day were all of a sudden facing up to 2,000 visits per second, overwhelming the servers hosting those websites. While it is difficult to gauge if there were casualties or deaths resulting from the attacks (e.g. in hospitals), the fact that some essential services, such as emergency services, were exposed suggests some lives may have been at risk. In the case of Georgia, which experienced a similar attack

[34] It is important to recognize that cyber space itself may raise security concerns as specific groups – such as terrorist organizations – might use it to communicate, fundraise, and recruit.

[35] Accessed on 6/10/2011 at http://csis.org/files/publications/101021_Significant%20Cyber%20Incidents%20Since%202006.pdf

[36] D. Verton, "Blaster worm linked to severity of blackout", ComputerWorld, 29 August 2003, accessed on 05/31/2012 at http://www.computerworld.com/s/article/84510/Blaster_worm_linked_to_severity_of_blackout. For economic cost calculations, see "The Economic Impacts of the August 2003 Blackout", prepared by the Electricity Consumers Resource Council (ELCON), 9 February 2004, accessed on 05/31/2012 at http://www.elcon.org/Documents/EconomicImpactsOfAugust2003Blackout.pdf

in August 2008 during its war with Russia, the societal impact was much more limited given the lower usage of cyber space services. The circumstances of war also downplayed the importance accorded to the cyber attack.

Third, there are other forms of attack beyond a DDoS which may affect national security. As shown in Table 5, several countries have been the victim of some form of organized cyber operations in the past few years. Many others are likely to have been targeted but are either aware of the organized incursions or do not want to draw attention to the fact that they have been targeted.

Table 5: Select Countries Targeted by Cyber Operations

Country	Attack Type	Date
Estonia	Distributed Denial of Service	April-May 2007
Lithuania	Distributed Denial of Service	June-July 2008
Georgia	Distributed Denial of Service	August 2008
South Korea	Distributed Denial of Service	July 2009
United States	Espionage	July 2009
Iran	Sabotage	July 2010
Internal censuring, e.g. China, Iran, Syria, Egypt	Restriction to Internet access	Multiple dates

As illustrated in Table 5, the United States suffered an attack in the summer 2009. Specifically, there was an intrusion into a US Department of Defense computer system that is thought to have compromised "terabytes" of technical information on the Joint Strike Fighter aircraft.[37] While no government services were compromised and no lives were lost, the cost of the stolen information is unfathomable and is likely to have substantial national security implications.

Currently, there is growing concern over cyber probes and penetrations that are routinely identified by computer security experts. Many of these probes are targeted at government networks and those of defence contractors, leading analysts to call the trend an "Advanced Persistent Threat".[38] According to General Keith Alexander, Head of US Cyber Command, the networks belonging to the US Department of Defense are probed about 250,000 times per hour – most of them seeming to be designed for network analysis and espionage.[39] A well-known probe was Ghostnet which mainly targeted embassies and the Tibetan diaspora.

[37] A terabyte represents a trillion bytes of information or 1,000 gigabytes.

[38] C. Ford, "National Security Challenges in Cyberspace", remarks delivered at the meeting of the Louisville Committee on Foreign Relations, Louisville, Kentucky, 21 September 2011.

[39] *Ibid*.

Revealed in 2009, Ghostnet penetrated some 1,300 computer systems around the world. Particularly disturbing was its ability to turn on the audio and webcams on several computers for spying purposes.

Fourth, countries that are subject to cyber operations or organized probes often cannot attribute the source of the attack. This in turn makes it difficult to gauge the intentions of the attacker and to formulate an appropriate response. The frequent inability to trace an attacker means that countries a) will not be in a position to take retaliatory measures and b) are unable to confirm whether or not an attack was done by a specific state actor or the result of a group working autonomously and not under direct political orders.

Beyond the frequent inability to identify the perpetrator(s) of an attack, there is limited international consensus on how to respond to a cyber attack – including how international law might apply. Can the country attack respond with the use of force if it has a good idea of who carried out the attack? How much force could be used and how should proportionality be established? From a different vantage point, should the state be held accountable for hosting an attacking party (in the event it had no knowledge of the existence and activities of this group on its territory)? These questions are examined in greater detail in Chapter 4.

Fifth, some countries may be concerned by the hardware or software installed in government computer systems. For example, given the complexity of today's microchips – which can pack several billion transistors – it is virtually impossible to guarantee that a microchip furnished by an unfamiliar provider does not contain remotely operated hidden backdoors or access points. This may be particularly sensitive for government agencies that to some degree depend on commercially available hardware technology. An oft-cited case is the restriction on French officials' use of BlackBerry devices in the summer 2007 over fear that their communications might be eavesdropped. In 2010, Germany followed suit by recommending that federal government employees not use BlackBerrys.

Lastly, it is also possible that computer systems are targeted physically. One feared, but not well understood possibility, is the use of an Electromagnetic Pulse (EMP) by an adversary to knock out computer and communications systems. An EMP may occur naturally as a result of solar flares, providing some indication of possible impacts. In 1859, a major solar storm that affected the earth's magnetic fields rendered telegraphs useless and burned several telegraph stations. A 2010 study by the Oak Ridge National Laboratory in the United States used a powerful solar storm in 1921 as a case study to understand the possible impact on the electricity grid. Assessed as a 1-in-100 year event, the study calculated that an equivalent solar storm would incapacitate or destroy up to "300 bulk power system transformers interrupting service to 130 million people for a period of years."[40]

The question is whether an actor could intentionally create an EMP to impact a country's access to cyber space. According to the Commission to Assess the Threat to the United States from EMP Attack, "[s]everal potential adversaries have or can acquire the capability to attack [...] with a high-altitude nuclear weapon-generated electromagnetic pulse". The effort level required does not seem to be major, as "a determined adversary can achieve an EMP attack capability without having a high level of sophistication."[41] Interestingly, the Commission notes that terrorist groups could be a potential source of EMP threats.

[40] See "Grid Cyber Security Act", 112 Congress, 1st Session, US Senate Report 112-34, 11 July 2011, p.26.

[41] J. Foster *et al.*, "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack", Vol.1, Executive Report 2004, accessed on 22/10/2011 at http://www.empcommission.org/docs/empc_exec_rpt.pdf

What Is Being Done to Address Cyber Security Challenges?

A host of measures are presently undertaken to address different types of cyber security challenges. The patchwork of measures can be organized into a matrix (see Table 6) which outlines preventive as well as consequence management measures. These in turn can be sub-divided according to technical and non-technical measures.

Table 6: Examples of Preventive and Consequence Management Measures

	Preventive Measures	Consequence Management
Technical Measures	Awareness raising Installation of protective software Use of black and white lists Use of open source software Introduction of new protocols (e.g. IPv6) Use of encryption	Increase bandwidth Filter incoming Internet traffic Block access to incoming Internet traffic Shift server usage Setting up "redundant" systems
Institutional Measures	Establish CERTs and CSIRTs Create specialized agencies / bodies (e.g. ENISA) Organize table top exercises (e.g. Cyber Storm) Introduce legislation and conventions Promote public-private partnerships Consider need for a national cyber security strategy	Set-up cyber "fire brigades" Promote national synergy vis-à-vis cyber security Engage in international cooperation Apply legislation

Preventive measures

Preventive measures serve to minimize cyber security risks. At the technical level, preventive means include raising awareness and identifying best practices to limit potential cyber threats. The installation of protective anti-virus software, using Domain Name System Security Extensions (DNSSEC), and migrating to Internet Protocol version 6 (IPv6) are all examples of proactive steps to boost security levels in cyberspace. While some of these measures will rest on the individual user, such as the installation of anti-virus software, many others will require action by Internet Service Providers, companies, and government organizations.

The advantages of many preventive measures, such as DNSSEC, are more likely to be visible when a large number of users adopt these technologies – effectively requiring extensive awareness raising. At the international level, the UN General Assembly has passed multiple resolutions to highlight defensive measures that governments can take to raise awareness, one of the latest being the December 2011 resolution 66/24 on Developments in the Field of Information and Telecommunications in the Context of International Security.[42]

Preventive measures at the institutional level tend to focus on the establishment of specific bodies or agencies that can provide early warning or disseminate best practices. Many countries now have a national Computer Emergency Response Team (CERTs) or Computer Incident Response Team (CSIRT) to serve as a coordinating centre or to monitor / receive information on unusual Internet activity.[43] They typically also have additional CERTs/CSIRTs that are hosted by a university or large IT company. Moreover, some countries have also developed cyber security strategies to identify the principal cyber issues of concern as well as possible means to address them. Most of these strategies are relatively recent, e.g. those of France (2011), Germany (2011), and Canada (2010).[44]

The United States has gone a step further in this direction by establishing a Cyber Command within the military command structure in May 2010.[45] According to William Lynn III, former US Deputy Defense Secretary, the US Department of Defense focus on cyber security began in earnest in 2008 when a US military laptop in the Middle East was infected via a flash drive. As the infection spread from one computer to the next, the intruder gained access to a network run by US Central Command. The incident resulted in the recognition that "passive defen-

[42] Examples of other relevant resolutions include: UN General Assembly Resolutions 53/70, 54/49, 55/28, 55/63, 56/19, 57/53, 57/238, 58/32, 58/199, 59/61, 60/45, 61/54, 62/17, 63/37, 64/25, 64/211, and 65/41. Several of these cover the topic of creating a global culture of cyber security (e.g. 58/199 and 64/211).

[43] For an indicative list, see http://www.codenomicon.com/resources/certs.shtml

[44] "Défense et sécurité des systèmes d'information: Stratégie de la France", Agence nationale de la sécurité des systèmes d'information, February 2011; "Cyber Security Strategy for Germany", Bundesministerium des Innern, February 2011; "Canada's Cyber Security Strategy", Public Safety Canada, 2010.

[45] The Command is now responsible for protecting all defence networks (e.g. the .mil domain name), supporting military and counter terrorism missions with a cyber dimension, and collaborating with partners outside the US government among others.

ces" such as firewalls and software patches were not enough to protect sensitive networks, and that a more systematic defence system would be necessary.[46]

Large-scale exercises to test the robustness of IT systems as well as procedures in case of an attack also fall under the umbrella of institutional measures of preventive nature. Among the largest exercises is the biannual Cyber Storm exercise organized in the United States. Cyber Storm III, which took place in September 2010, engaged seven US cabinet level departments including Commerce, Defense, Energy, Homeland Security, Justice, Transportation, and Treasury. The White House, as well as representatives from the intelligence community, were also engaged in the exercise. Twelve other countries as well as eleven US states also took part in the exercise.[47] Demonstrating the importance of the private sector in this domain area, 60 private sector companies took part in the exercise which served to test organizations abilities to prepare for, recognize, protect from, and respond to a cyber attack.[48]

Larger-scale exercises are also taking place in Europe, albeit at a slower pace. In November 2010, the EU organized its first pan-European exercise on critical information infrastructure protection. Known as Cyber Europe 2010, it was executed by the European Network and Information Security Agency (ENISA). The exercise was based on a fictitious scenario simulating approximately 300 hacking attacks seeking to undermine Internet connectivity, including online services across Europe. Among the principal lessons coming out of the exercise is the need for increased cooperation among EU Member States and the importance of engaging the private sector to strengthen cyber security. The final report also notes "that the procedures on how to handle cyber incidents do not yet exist on a pan-European level. Such procedures need to be identified and tested in future such exercises."[49]

International organizations also conduct periodic exercises to test their cyber defences. In the security area, NATO engages in several different exercises. Examples range from the Cyber Coalition exercises held in 2010 and 2011 to test NATO's procedures for responding to large scale cyber attacks that target its information structures to specialized exercises organized by the NATO Coopera-

[46] W. J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy", *Foreign Affairs*, Vol.89, No.5, September-October 2010.

[47] The international partners were Australia, Canada, France, Germany, Hungary, Japan, Italy, the Netherlands, New Zealand, Sweden, Switzerland, and the United Kingdom.

[48] See "Cyber Storm: Securing Cyber Space", Department of Homeland Security, accessed on 5/11/2011 at http://www.dhs.gov/files/training/gc_1204738275985.shtm. For the final exercise report, see http://www.dhs.gov/xlibrary/assets/nppd-cyber-storm-iii-final-report.pdf

[49] Cyber Europe 2010 – Evaluation Report, European Network and Information Security Agency (ENISA), 2011, p.8, accessed on 16/12/2012 at http://www.enisa.europa.eu/media/press-releases/eu-agency-enisa-issues-final-report-video-clip-on-cybereurope-2010-the-1st-pan-european-cyber-security-exercise-for-public-bodies

tive Cyber Defence Centre of Excellence based in Tallinn, Estonia (e.g. Baltic Cyber Shield Cyber Defence Exercise 2010).

Lastly, many governments are exploring ways to engage more closely with the private sector to strengthen the protection of critical infrastructures. Recognizing that the private sector largely owns critical infrastructures (e.g. water, sewage, electricity) and often has advanced know-how on how to protect networks, the movement towards public-private partnerships is likely to increase over time. An example is the US Enduring Security Framework, whereby the chief executive officers and chief technology officers of principal IT and defence companies periodically get to meet with senior officials from the Department of Homeland Security, the Department of Defense, and the Office of the Director of National Intelligence to discuss cyber issues of concern.[50]

Consequence management measures

Consequence management measures focus on mitigating the effects of a cyber operation while it is on-going or putting measures in place in the immediate aftermath. During the DDoS attack on Estonia in 2007, technical experts took a number of steps to minimize the effects of the attacks. These ranged from increasing available bandwidth so legitimate Internet traffic could reach its destinations in Estonia to filtering incoming traffic to limit the number of visits to specific websites. Estonian information technology experts also were in close contact with their peers in neighbouring countries to get a better sense of the volume of incoming Internet traffic and whether additional measures – such as blocking access – could be done from outside Estonia. These efforts were spearheaded by the CERT Estonia with the support of system administrators inside and outside Estonia.[51] In any other attack of similar nature, it is likely that the victim country would engage in similar technical measures.

Among the more novel consequence management measures currently under consideration is the value of having “cyber fire brigades”, “cyber defence leagues”, or “cyber militias”. Building on the CERT model, such groups would be made up of voluntary individuals – most of which with specialist background in IT. Besides sharing knowledge in advance of a cyber event, such groups would make their services available if needed during a cyber attack. In such circumstances, their roles could be wide-ranging, from trying to pinpoint the origin of the attack to devising protective measures. Such bodies could also serve to reinforce or support

[50] Lynn III, “Defending a New Domain: The Pentagon’s Cyberstrategy”, *op.cit.*

[51] For more information on the cyber attack on Estonia, see E. Tikk, K. Kaska, and L. Vihul, *International Cyber Incidents: Legal Considerations*, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2010.

the work of national CERTs and CSIRTs that might be overwhelmed in the early stages of a cyber attack. Estonia has already developed a cyber defence league which consists of approximately 100 information technology experts.

Since cyber operations can take many different guises, consequence management measures need to be flexible. In many cases, raising awareness – which is an important component of prevention – helps individuals and organizations take the necessary steps to avoid becoming the victim of known threats. For example, those working with sensitive data need to be aware of the dangers of introducing external hardware, such as a thumb drive, into their computer systems. Doing so may introduce malware which is hard to protect against with anti-virus software or firewalls. To limit the possibilities of espionage, individuals and organizations may need to disconnect several of their computer systems from the Internet. Critical infrastructure operators may need to rethink how their control systems are accessed and operated – including their reliance on commercially available operating systems. Identifying measures such as these typically become more evident after a cyber incident.

At the institutional level, countries and international organizations use the lessons identified from recent cyber attacks to create new international instruments – mainly of legal nature – to limit the scope for similar cyber incidents in the future. Organizations and bodies engaged in such activity include the CoE, the EU, the G8, the International Telecommunication Union (ITU), the OECD, the Organization for Security and Cooperation in Europe, and the United Nations. Examples of such measures by the EU include the 2009 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience".[52] Among others, the communication outlines specific ways in which the EU should improve EU-level cooperation and coordination in the area of critical information infrastructure protection.

To improve consequence management capacity over time, countries are also reviewing their internal mechanisms to better calibrate cooperation across different government departments and agencies that may be engaged in response to a cyber attack. As was the case for preventive measures, this also includes building cooperative ties with the private sector, non-profit sector, other countries and international organizations.

[52] Accessible at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0149:EN:NOT. For a fuller overview of these instruments, see E. Tikk, *Frameworks for International Cyber Security*, Legal and Policy Documents, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, May 2010.

What Are the Outstanding Issues?

Looking ahead, policymakers face several issues that require continued consideration. Beyond the overarching need to continue raising awareness, at least three themes stand out.

Reaching balance between defensive and offensive cyber capabilities

Traditionally, there was limited incentive for countries to pursue offensive cyber capabilities beyond those associated with traditional military tasks such as jamming military assets in the battle space. The principal reason is that a move towards offensive cyber capabilities would encourage a cyber arms race which in the end would be difficult to monitor by the participating states.

While it is still not a topic for public discussion, there currently seems to be greater appetite among countries for offensive cyber capabilities. Frequently, they are said to complement military capacity and only to be used in time of armed conflict. It comes as no surprise that cyber space is sometimes referred to as the fifth domain of war fighting. According to a preliminary assessment carried out by the CSIS, 33 countries include cyber warfare in their military planning and organization. These might include "cyber capabilities for reconnaissance, information operations, the disruption of critical networks, for 'cyberattacks', and as a complement to electronic warfare and information operations."[53] Among the countries in the list are Albania, Austria, Belarus, Brazil, Canada, China, the Democratic People's Republic of Korea, Denmark, Estonia, Finland, France, Germany, India, Israel, Iran, Myanmar, the Netherlands, the Republic of Korea, Russia, Switzerland, the United Kingdom, and the United States.[54] The study also notes that an additional 36 countries have well developed defensive capabilities that could be translated into offensive capabilities if desired.[55]

[53] J. Lewis and K. Timlin, "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization", CSIS, Washington, DC, 2011. William Lynn (former US Deputy Secretary of Defense) offers a similar figure for the number of countries pursuing offensive cyber capabilities. See W. J. Lynn III, "The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack", *Foreign Affairs*, Vol.90, No.5, September 2011.

[54] For the full list, see *ibid.* (Lewis and Timlin), pp.5-22.

[55] *Ibid*.

A possible trend towards offensive cyber weapons raises important questions. For example, might it facilitate cyber operations in future conflict and warfare? Such deliberations are not new. When NATO intervened in Libya, US policymakers pondered on whether or not a cyber attack should be part of an overall strike on Libya. The aim of the cyber offence would have been to dismantle the Qaddafi government's air defence system. In the end, officials decided not to use such an approach for fear that it might set precedent for other nations such as Russia and China to use similar tactics in the future.[56] Further ahead, it may not be easy to constrain the use of cyber capabilities, as a cyber dimension is likely to become a strategic enabler in conflict situations.

A shift in the balance between defensive and offensive cyber capabilities may also have implications for which departments or agencies are in the lead with respect to cyber security. A principal issue at stake is the division of labour between military and civilian agencies. In the United States, there already have been divisions over whether such a role would go to the Department of Defense or the Department of Homeland Security. General Keith Alexander's confirmation process, which lasted for over half a year, suggested some hesitancy towards double-hatting the head of the National Security Agency as the head of Cyber Command. "Securitizing" cyber space and giving a greater role to the military is likely to raise questions such as the implications for general accessibility to cyber space in times of conflict. A rise in offensive cyber capabilities also raises the question of the role of cyber power vis-à-vis national security. According to Joseph Nye, cyber power may eventually follow in the footsteps of other forms of power that have dominated at different points in time (sea power, air power, space power).[57] If this is indeed the case, policymakers will need to think through how such power is to be utilized under a range of different scenarios.[58]

Overall, while reaching clarity on some of these issues – such as the pursuit of offensive cyber capabilities – will rest mainly with individual countries, many will require international dialogue to move forward (e.g. agreement on cyber concepts) – requiring careful deliberations across stakeholders.

[56] See E. Schmitt and T. Shanker, "US Debated Cyberwarfare in Attack Plan on Libya", *The New York Times*, 17 October 2011.

[57] J. Nye, "Power and National Security in Cyber Space", in K. Lord and T. Sharp (eds.), *America's Cyber Future: Security and Prosperity in the Information* Age, Vol.2, Center for a New American Century, Washington, DC, June 2011.

[58] For additional views on possible futures of cyber conflict and cooperation see J. Healy, "The Five Futures of Cyber Conflict and Cooperation", Atlantic Council, Washington, DC, IssueBrief, Cyber Statecraft Initiative, December 2011.

Clarifying the legal landscape and the application of international law

While there is an international convention on Cybercrime (2004), several directives and communications by international organizations on issues relating to cyber space, and numerous legal studies on cyber operations and international law, there are many questions that require additional reflection.[59]

Exacerbating the challenge of clarifying the legal landscape are national divergences over key cyber concepts. Presently, terms such as cyber terrorism, cyber war, cyber hostilities, and cyber warfare have no agreed definitions for the purposes of law. The ability to reach some kind of agreement on definitions is important as it may determine whether or not certain national and international law-enforcement agencies can have a role in pursuing the perpetrators of such attacks (contingent on being identifiable). For example, cyber vandalism and cyber hooliganism fall under the wider definitional umbrella of cyber crime. As such, law enforcement and existing legal conventions such as the Council of Europe Convention on Cybercrime can apply in such cases.[60]

Efforts at the UN and international level, for example via meetings of the UN Group of Governmental Experts (GGE), have yet to produce tangible results.[61] Since its establishment in 2009, the GGE has met four times and will meet again during 2012. It has covered a range of topics including best practices, capacity building measures for developing countries, confidence building measures, and the elaboration of common cyber-related definitions. Still, limited progress was achieved concerning shared concepts and norms.

With respect to the application of international law, several issues remain nebulous. In the area of law governing the resort to force between states (also known as *jus ad bellum*), a principal issue is whether or not a cyber operation can be equated to an "armed attack", a wrongful threat or use of "force", or a "threat to

[59] With respect to studies, see for example C. Czosseck and K. Geers (eds.), "The Virtual Battlefield: Perspectives on Cyber Warfare", *Cryptology and Information Security Issues*, Vol.3, IOS Press, Amsterdam, The Netherlands, 2009; N. Melzer, "Cyberwarfare and International Law", UNIDIR Resources, Geneva, 2011; M. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law*, Vol.37, 1999; M. Schmitt, "Cyber Operations and the *Jus in Bello*: Key Issues", *Naval War College International Law Studies*, Vol.87, 2011.

[60] See the special report by the *Economist Technology Quarterly* published on 6 December 2008.

[61] Members of UN GGE come from member states and typically consist of topic experts selected on the basis of equitable geographical distribution. GGE's have been formed to examine diverse issues such as Certain Conventional Weapons, illicit brokering in small arms and light weapons, and the relationship between disarmament and development security.

international peace and security".[62] While it is generally agreed that cyber attacks with effects similar to those resulting from chemical, biological, nuclear, or kinetic weaponry would fall under the prohibition of Article 2(4) of the UN Charter, the challenge is how to classify attacks that do not directly cause death, injury or destruction.[63] In addition, there is no clear understanding of the precise threshold at which a cyber operation could be classified as a wrongful threat / use of "force" or an "armed attack".[64] For example, could a cyber attack on a critical infrastructure be considered an "armed attack" under the auspices of the UN Charter?

Although there are differing opinions on how cyber operations relate to terms such as the use of force, most legal experts agree that International Humanitarian Law (IHL, also known as the law of armed conflict / *jus in bello*) is applicable to cyber operations executed within the context of an international or non-international armed conflict.[65] Partially, this is due to the fact that IHL is flexible to accommodate new technological developments such as those presented by the cyber domain (e.g. via the Martens Clause implied by Article 36 of Additional Protocol I).[66] While cyber operations may be justifiable under IHL, the application of cyber operations should ideally be proportional and targeted to military assets to limit the impact on civilians. However, given the dual use of many critical infrastructures (water plants, electricity) that are needed by the military to sustain its efforts, it could be argued that cyber attacks could legally be applied to a wide range of infrastructures.

The range of responses available to victims of a cyber operation also requires further reflection. Since most cyber activities with a national security dimension tend to focus on espionage and intelligence gathering, they fall outside the scope of IHL. Even in the case of a DDoS attack, Article 41 of the UN Charter notes that the interruption of communication may be considered a "measure not involving

[62] Cyber operations are sometimes categorized as a computer network attack (symbolizing a more offensive use of cyber capabilities), computer network exploitation (e.g. espionage), or computer network defence (symbolizing a more defensive use of cyber capabilities).

[63] Article 2(4) of the UN Charter states that "[a]ll members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations".

[64] See N. Melzer, "Cyberwarfare and International Law", *op.cit.*, p.12.

[65] *Ibid*.

[66] See R. Geiss, "The Legal Regulation of Cyber Attacks in Times of Armed Conflict", Proceedings of the Bruges Colloquium, Technological Challenges for the Humanitarian Legal Framework, 21-22 October 2010. For information on the Martens Clause, see R. Ticehurst, "The Martens Clause and the Laws of Armed Conflict", *International Review of the Red Cross*, No. 317, accessed on 05/31/2012 at http://www.icrc.org/eng/resources/documents/misc/57jnhy.htm. The Additional Protocol I refers to the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 8 June 1977.

armed force" – suggesting such an attack might not fall under the prohibition of Article 2(4).[67]

Even in cases were international law might apply, the concept of self-defence may prove restrictive given the principles of necessity and proportionality. If these modalities are to be followed, "self-defensive action in cyberspace is not permissible in response to harm which has already been caused by hostile cyber operations, but only with a view to preventing or repelling an imminent or ongoing attack…"[68] Given these constraints, policymakers will need to carefully examine options that might be at their disposal in the event of a cyber operation that affects national security – even if it does not lead to death, injury, or destruction. Given the difficulties of attribution as well as limitations with respect to self-defence, policymakers will need to think "out of the box" to gauge the applicability of tools – including those outside the cyber realm.

Making progress on a governance model

An issue gathering momentum is whether or not a more formal governance model is needed to manage the Internet. Among policymakers, three principal views are discernible. First, those who think that the current model works well and there is no need for greater Internet oversight (e.g. a position commonly held by US policymakers). Second, those who think that the present model is no longer viable and there is need for greater oversight via an international body (e.g. Brazil, China, India, Russia, and South Africa). Third, those who would like to see more binding rules for behaviour in cyber space, e.g. through an international treaty, convention, or code of conduct with an emphasis on regulating military cyber applications (e.g. China, Russia).[69]

For those seeking a greater government role, there are suggestions that the ITU – the UN specialized agency for information and communication technologies – take on the role of overseer of Internet policy and its development. It has already taken some initiatives in this area by organizing the Internet Governance Forum and the World Summit of the Information Society. The ITU is now also conducting a review of international arrangements governing telecommunications and may aim to expand its regulatory authority at a summit planned for December 2012 in Dubai.[70]

[67] Melzer, "Cyberwarfare and International Law", *op.cit.*

[68] *Ibid.*, p.18.

[69] It should be noted that there are international non-governmental bodies that assist with the development of the Internet. Among the better known is the Internet Corporation for Assigned Names and Numbers (ICANN) which coordinates the Internet's naming system. At the technical level, a less well known entity is the Internet Engineering Task Force that serves as the main standards setting organization for the Internet.

[70] V. Cerf, "Keep the Internet Open", *The New York Times*, 24 May 2012, accessed on 05/31/2012 at http://www.nytimes.com/2012/05/25/opinion/keep-the-internet-open.html

Some countries are proposing more binding rules or code of conducts. For example in September 2011, China, Russia, Tajikistan, and Uzbekistan submitted an International Code of Conduct for Information Security as a formal document of the 66th session of the UN General Assembly for deliberations. The document was specifically formulated as a potential General Assembly resolution.[71] Among others, the Code of Conduct calls for the "establishment of a multilateral, transparent and democratic international Internet management system to ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet".[72]

Another option circulated for consideration is the establishment of a convention for information security. The aim of such a convention would be to identify which type of behaviour is unacceptable in cyber space. In September 2011, the same month the International Code of Conduct was presented; Russia also forwarded a concept for a UN Convention on International Information Security. Besides offering definitions of key terms such "information security" and "information warfare", the document outlines principles for ensuring international information security and measures for averting military conflict in the information space.[73]

As shown in Table 7, each option has its own advantages and drawbacks. For example, keeping an open Internet to the extent possible (option 1) is seen to promote innovation and economic prosperity. On the other hand, limited governance may at some point encourage some countries or organizations to create "gated" communities over which they impose their rules – for example on the degree of assurance and attribution imposed on users to enter those communities. With respect to option 2, which could entail greater Internet oversight via an international body such as the ITU, a benefit could be greater engagement by individual countries in enhancing Internet access and security. As most countries are members of the ITU, they would have a stake and ownership in the process, ideally promoting measures with strong backing and support. On the other hand, such a move could just as easily lead to stalemates as countries disagree on the appropriate levels of oversight, hampering the ability of an international organization to manage the Internet.

[71] See "Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General", UN General Assembly A/66/359, 14 September 2011, accessed on 05/31/2012 at http://isocbg.files.wordpress.com/2011/09/un-information-secutiy-code-ru.pdf

[72] *Ibid*., p.4.

[73] "Convention on International Information Security", Russian Security Council and Russian Ministry for Foreign Affairs, available at http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument

Table 7: Summary of Principal Internet Governance Options

Option	Advantages	Disadvantages
Option 1 – Status quo (no additional oversight)	Has a good track record, especially with respect to promoting economic and commercial activities Likely to promote new applications and uses for the Internet May eventually encourage the development of norms to guide state behaviour in cyber space	May in the long term not provide enough protection / security to Internet users May over time encourage "gated" communities in which some countries impose their own governance mechanisms
Option 2 – Oversight by an international body	Might facilitate the identification of "unacceptable" cyber behaviour May produce a more secure Internet as countries have a greater stake / role via an international body	Divisions over the role of an international body in specific areas could undermine the efficiency and openness of the Internet Privacy and anonymity online could be curtailed
Options 3 – Setup of "binding rules" for behaviour	Could lower the risks for an "arms race" in cyberspace, especially if binding rules go beyond Internet governance Could provide a good starting point for identifying some basic codes of conduct	Difficulty of verifying that no military applications are being developed Overcoming attribution and definitional challenges, such as what constitutes a cyber weapon Complicating verification processes

Since the options are not mutually exclusive, policymakers may eventually follow a route that incorporates elements from the different options. For example, if there is a desire for more control over the Internet, it could be feasible to have both an international oversight body complemented by international agreements concerning acceptable cyber behaviour. Some may push for countries to assume responsibility for cyber activities on their territory, effectively making them responsible in case an attack is launched from their national boundaries.

Regardless of the direction taken, the impacts will be substantial. Future policy decisions in this arena will affect numerous domains, including levels of anonymity on the Internet, the evolution of cloud computing, and levels of international cooperation. And while there is no right answer, at heart of these deliberations will be how to best balance individual freedoms on the Internet while guaranteeing a standard level of security for users.

Conclusion

While there are still very diverging views on the importance of cyber security, it is clear that the cyber dossier will increasingly be on policy- and decision makers' agendas. As this paper has suggested, several findings can be highlighted.

First, there are many reasons why policymakers should care about cyber space. These range from a growing number of Internet users to the growing ease with which an actor can acquire and customize malicious software. It is also evident that countries themselves may be victimized by cyber operations. While the effects of a cyber operation may hardly be noticeable, the losses, in terms of intellectual property, could be extensive. With this in mind, it is important not to exaggerate the cyber threat vis-à-vis national security. While there are predictions of cyber wars or cyber warfare, it is more likely that we will see cyber tools applied in times of conflict as an enabler. The adage "cyber in war" rather than cyber war is probably accurate, so policymakers should avoid aggrandizing the cyber threat.

Second, there are a number of measures that nations and the international community can take to minimize the risk of cyber challenges. These include both technical and institutional means that can be applied in a preventive and consequence management situation. Key among these measures is to continue raising awareness of risks in cyber space and engaging in international cooperation.

Finally, there are several cyber-related issues that will need continued consideration in the future. While there are no easy answers, policymakers and legal experts will have to grapple with the legal aspects of cyber security and reflect on whether or not a more formalized system is needed to increase Internet governance. Regardless of the path taken, the choices will have longstanding implications for cyber security and how cyber space is used in the future.

Annex A
Glossary of Technical Terms

The definitions used below are based on the *Tech Terms Computer Dictionary* authored by Per Christensson. These can be found at www.techterms.com

The sole exceptions are the definitions for “blended threat”, “hacktivist”, and “script kiddie” which are based on information provided on the online encyclopaedia of PC Magazine. These are accessible at http://www.pcmag.com/encyclopedia/

Word / Term	**Definition**
Blended Threat	Malicious software that may combine elements of a virus, worm, Trojan horse, or other malicious code.
Botnet	A botnet is a group of computers that are controlled from a single source and run related software programs and scripts. While botnets can be used for distributed computing purposes, such as a scientific processing, the term usually refers to multiple computers that have been infected with malicious software. A hacker may create a botnet for several different purposes, such as spreading viruses, sending e-mail spam, or crashing Web servers using a denial of service attack.
Botnet Operator	Refers to the individual in control of a botnet. Sometimes also known as botnet herders.

DDoS Attack

A denial of service attack is an effort to make one or more computer systems unavailable. It is typically targeted at web servers, but it can also be used on mail servers, name servers, and any other type of computer system.

A distributed denial of service attack tells all coordinated systems to send a stream of requests to a specific server at the same time. If the server cannot respond to the large number of simultaneous requests, incoming requests will eventually become queued. This backlog of requests may result in a slow response time or a no response at all. When the server is unable to respond to legitimate requests, the denial of service attack has succeeded.

Firewall

A computer firewall limits the data that can pass through it and protects a networked server or client machine from damage by unauthorized users. Firewalls can be either hardware or software-based.

Hacktivist

Combining the term hacker and activist, hacktivists use computers and networks to demonstrate or protest against a company or government agency. Examples of hacktivist activities include trying to bring down a website or gaining unauthorised access to a computer network.

Rootkit

A rootkit is a software program designed to give the user administrator access to a computer without being detected. Rootkits often work by exploiting security holes in operating systems and applications. Others create a “back door” login to the operating system, which allows a user to bypass the standard login procedure when accessing a system.

Script Kiddie

A computer novice who illegally tries to gain access to a computer system using programs (scripts) written by others.

Trojan Horse

Trojan horses are software programs that masquerade as regular programs, such as games, disk utilities, and even antivirus programs. If activated, these programs can do malicious things to the targeted computer. Trojan horses do not replicate themselves; however, it is possible for a Trojan horse to be attached to a virus file that spreads to multiple computers.

Virus

Computer viruses are small programs or scripts that can negatively affect the performance of a computer. They can create files, move files, erase files, consume a computer's memory, and cause the computer not to function correctly. Some viruses can duplicate themselves, attach themselves to programs, and travel across networks.

Worm

A computer worm is a type of virus that replicates itself, but does not alter any files on the machine. However, worms can still cause problems by multiplying so many times that they take up all of a computer's available memory or hard disk space – effectively slowing down its performance or crashing it. Unlike viruses and Trojan horses, worms can replicate themselves and travel between systems without any action from the user.

Geneva Papers — Research Series

No.1 — 2011 G.P. Herd, “The Global Puzzle: Order in an Age of Primacy, Power-Shifts and Interdependence”, 34 p.

No.2 — 2011 T. Tardy, “Cooperating to Build Peace: The UN-EU Inter-Institutional Complex”, 36 p.

No.3 — 2011 M.-M. Ould Mohamedou, “The Rise and Fall of Al Qaeda: Lessons in Post-September 11 Transnational Terrorism”, 39 p.

No.4 — 2011 A. Doss, “Great Expectations: UN Peacekeeping, Civilian Protection and the Use of Force”, 43 p.

No.5 — 2012 P. Cornell, “Regional and International Energy Security Dynamics: Consequences for NATO’s Search for an Energy Security Role”, 43 p.

No.6 — 2012 M.-R. Djalili and T. Kellner, “Politique régionale de l’Iran : potentialités, défis et incertitudes”, 40 p.

No.7 — 2012 G. Lindstrom, “Meeting the Cyber Security Challenge”, 39 p.

Newidea - 01.2012

GCSP
avenue de la Paix 7bis
P.O. Box 1295
CH - 1211 Geneva 1
T +41 22 906 16 00
F +41 22 906 16 49
info@gcsp.ch
www.gcsp.ch

GCSP
Geneva Centre for Security Policy
Centre de Politique de Sécurité, Genève
Genfer Zentrum für Sicherheitspolitik

Impartial, Inclusive, Influential