DCAF HORIZON 2015 WORKING PAPER No. 1

DEMOCRATIC GOVERNANCE CHALLENGES OF CYBER SECURITY

Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler

GENEVA
SECURITY FORUM

10
DCAF

DCAF HORIZON 2015 WORKING PAPER No. 1

DEMOCRATIC GOVERNANCE CHALLENGES OF CYBER SECURITY

BENJAMIN S. BUCKLAND, FRED SCHREIER, THEODOR H. WINKLER

GENEVA SECURITY FORUM

10 DCAF

Table of Contents

Abstract

Cyber security encompasses borderless challenges, while responses remain overwhelmingly national in scope and even these are insufficient. There are enormous gaps in both our understanding of the issue, as well as in the technical and governance capabilities required to confront it. Furthermore, democratic governance concerns – particularly regarding control, oversight and transparency – have been almost entirely absent from the debate. These concerns are exacerbated by the enormous role played by private actors (both alone and in cooperation with governments) in online security of all types. Given the pace at which states and private companies are reinforcing online security and preparing for cyber war, addressing democratic governance concerns has never been more pressing. They are the primary subject of this paper.

Introduction

Cyberspace has many competing definitions. However, for the purposes of this paper, it is defined *as the interdependent network of information technology infrastructures*. It includes the internet, telecommunications networks, computer systems and embedded processors and controllers in various industries.[1]

The past two decades have seen an explosion in the reliance of just about everyone on network connectivity. The growth of the internet has been characterised by an emphasis on interoperability, efficiency and freedom but our growing reliance has not been matched by efforts to keep it secure. This reflects the original purpose of the web, which was to exchange scientific data, rather than to (as now) support an entire global economy. An explosion of use and functionality (for both good ends and bad) has outpaced efforts to reform and secure the original infrastructure.[2]

Cyber (or online—the terms are here used interchangeably) security encompasses borderless challenges, while responses remain overwhelmingly national in scope and even these are insufficient. There are enormous gaps in both our understanding of the issue, as well as in the technical and governance capabilities required to confront it. Furthermore, democratic governance concerns—particularly regarding control, oversight and transparency—have been almost entirely absent from the debate. These concerns are exacerbated by the enormous role played by private actors (both alone and in cooperation with governments) in online security of all types. Given the pace at which states and private companies are reinforcing online security and preparing for cyber war, addressing democratic governance concerns has never been more pressing. They are the primary subject of this paper.

As the discussion below makes clear, there is a great deal of diversity in the types of online threat, as well as in the actors involved. When looking at the issue from the perspective of transparency, control and oversight, however, the various threats can be divided into two main types.

States are, of course, particularly concerned with national security and the possibility that states or non-state actors or groups will steal, change, destroy and otherwise compromise critical information and information infrastructures. Of particular national security concern is the threat of disruption to telecommunications, electrical power, energy pipelines, refineries, financial networks, health systems and other essential services.[3] The case of Estonia (see Box 3.) demonstrates that such concerns are not unfounded and many have gone as far as to claim that cyber war,

[1] The authors would like to thank Tobias Bolliger, Belinda Cleeland, Anja Ebnöther, Paul Meyer, Daniel Stauffacher, Barbara Weekes and Aidan Wills for their helpful and insightful comments on the text. In particular, DCAF would like to thank the Geneva Security Forum for its substantive contribution and partnership in the preparation of this paper.

[2] Lloyd's Emerging Risks Team, *Digital Risks: Views of a Changing Risk Landscape* (London: Lloyds, 2009).

[3] White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington DC: White House, 2009).

as this type of threat can be broadly called, will change war fighting as dramatically as the introduction of other new technologies has done in past.[4] It may indeed be argued that cyber war will herald a second wave of the revolution in military affairs and replace kinetic energy as the main agent of warfare. Cyber war raises questions related to what constitutes critical infrastructure, what constitutes an attack, and what role the security sector can or should play in defence or counter-attack. As we point out below, cyber war has blurred both (civil and military) categories of target as well as categories of attacker. There are thus serious questions about what, in the event of a major cyber war, states are able to credibly and legally threaten – diplomatic demarche, formal protest, economic retaliation, criminal prosecution, or military strike.[5]

More important still is the question of what democratic processes or legal standards might govern any decision to respond. This last point is particularly important given that a number of factors dramatically reduce the transparency of cyber war vis-à-vis other types of conflict. These will be dealt with in more detail in the final section of the paper. However, it is worth mentioning a couple of them at the outset. Firstly, there is seldom much fire and smoke to indicate that an online attack has occurred—technical and highly specialised knowledge is required for detection, identification and retaliation, as is the cooperation of private actors. This reduces transparency enormously. A large-scale attack or counter-attack could thus occur without an oversight body (the relevant parliamentary committee, for example) ever becoming aware of the fact. In addition, because of the highly technical nature of the problem, the role of intelligence agencies (vis-à-vis law enforcement actors) is amplified, something that further reduces transparency and opportunities for oversight.

Today, challenges to national security and to critical national infrastructure (broadly defined) still form only a small part of the overall threat landscape. A much larger problem, and thus a particular focus of this paper, is the question of how to ensure democratic oversight over internet regulation and the use of online infrastructure to target individuals and other actors. Thus, the concern is not so much with cyber war or the online vulnerability of national infrastructure but with issues such as censorship, warrantless surveillance of email traffic or the gathering and retention of private data by IT firms (often at the behest of, and in cooperation with, governments).

In this way, discussions of online security parallel debates that have taken place in a number of other security domains about the tension between national security and what has been dubbed "human security." This balance—between state security and human security is neatly encapsulated within the key tension at the heart of cyber security, although here the third imperative of what we might call "private security"—the security of corporations and private companies—is added to the mix.

[4] John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Washington DC: RAND, 1997).

[5] John Markoff, David E. Sanger and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *New York Times,* 25 January 2010, World section.

Cyber security presents us with a threefold challenge. There is the dual (and sometimes complimentary) challenge of promoting both public and private security by securing IT networks and defeating the criminal and violent groups that use them to pursue their aims. These are challenges which require the building of comprehensive mechanisms for public private cooperation. Equally, however, cyber security represents a growing challenge to democratic governance, as public and private efforts to secure IT networks and monitor the traffic that they carry must be balanced with human security concerns and, in particular, with human rights to privacy and to freedom of expression and association.

The discussion that follows is thus divided into two main sections. Section one takes a brief look at the major threats and relevant actors, with a particular focus on public private cooperation. Section two then focuses on the key question of democratic governance and is divided into sub-parts on oversight, on human rights protection and, finally, on possible democratic governance issues related to cyber war.

1. Threats and Actors

1.1 Threats

One particular feature of cyber security is that it is often extremely difficult to accurately identify the perpetrators of an attack or (often) even its country of origin. It is thus relatively easy for one or a group of perpetrators to mask their involvement or otherwise disguise themselves as another user.[6] This issue will be revisited below but, setting identification issues aside for the moment, the two tables that follow outline what are, in general terms, the key sources and objectives of online threats.

1.2 Actors

One of the key challenges of cyber security—and an aspect that has made it of particular interest to the Horizon 2015 project—is the fact that, while governments generally have some degree of overall *responsibility* for information and communications networks, such networks are primarily *owned* by private actors.[7] As this paper goes on to discuss below, this involvement significantly complicates the dual challenge of security and democratic governance. In particular, these two sets of actors have specific concerns that hinder both the efficiency and efficacy of cyber security efforts, as well as undermine attempts to protect fundamental rights and freedoms.

These difficulties are amplified by the global nature of both the problem and its solutions. Here, there is a role for international actors in the development of global standards and in the identification of best practices. Such actors can also play a role in encouraging the harmonisation of national laws on investigation and prosecution, data preservation, protection, privacy, approaches to network defence and response to attacks. In addition, international actors can play a role in identifying oversight deficits and in identifying best practice in democratic oversight of online security actors and partnerships. This area merits substantially more attention, given that current international attempts to identify best practice (by, for example, the G8's Subgroup on High-Tech Crime, the UN Congress on Crime Prevention and Criminal Justice or the CoE Octopus Conference on Cooperation Against Cybercrime), have mostly focused on effectiveness, rather than on transparency or oversight, an issue that will be revisited below.

These last few points are particularly important given the large disparities that exist in terms of both the technological capacities and the legal frameworks between different states. While many states, such as the US and the UK, are pouring millions into cyber security and rapidly developing legislation on the issue, others lack even

[6] Markoff, Sanger and Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent"

[7] Jennifer Wood and Benoît Dupont, eds., *Democracy, Society and the Governance of Security* (Cambridge: Cambridge University Press, 2006).

basic IT infrastructure, let alone strategies for dealing with the cyber-related threats that both target and emanate from their territories. There is thus a need to develop laws relating to cyber-security (including proper democratic oversight) and covering cyber-crimes. Where both capacity and relevant legislation is lacking, cyber crimes become difficult, if not impossible, to investigate or prosecute, while an absence of properly constituted oversight bodies makes violations of the rights to freedom of expression, privacy and freedom of association all the more likely.

Relevant international instruments include: the United Nations General Assembly resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on "Combating the criminal misuse of information technologies"; "Guidelines for the cooperation between law enforcement and internet service providers against cybercrime," adopted at the global conference "Cooperation against Cybercrime" held in Strasbourg on 1–2 April 2008 and, at the regional level, the Council of Europe Recommendation No. R (89) 9 on Computer-Related Crime and the European Convention on Cybercrime, which requires member states to adopt legislative measures to establish the powers and procedures for criminal investigations regarding criminal conducts committed through the use of computer systems, and the collection of electronic evidence.

International and regional human rights instruments are also relevant, including: the *International Covenant on Civil and Political Rights* (particularly article 17 on the right to privacy, article 19 on freedom of expression and article 22 on freedom of association), the *European Convention on Human Rights*, the *African Charter on Human and Peoples' Rights* and the *American Convention on Human Rights*. International and regional organisations have also sought to address electronic data protection more specifically, through measures and instruments such as: the *UN General Assembly Guidelines for the Regulation of Computerized Personal Data Files* and the *Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data,* which, in particular, reiterates protections related to privacy and freedom of expression with regards to electronic data and correspondence.

The public is another crucial element and there is a clear need to engage them through education campaigns that promote awareness of fraud, identity theft, predators, and ethics, as well as of their relevant rights.

The third of the tables below outlines some of the key actors involved in responding to online threats.

Table 1. Sources of Cyber Threats[8]

Threat source	Description of Threat
States	Foreign intelligence services use IT tools for information gathering and espionage. This may be aimed at other states (both friendly and hostile), or at non-state threats. States may also target foreign adversaries for the purposes of disinformation, destablisation, intimidation, or even full-scale cyber war. From a human security standpoint, states may also constitute a threat through their capture and use of personal data, in some cases without judicial warrant or adequate democratic oversight.
Corporations	Businesses and corporations (sometimes in collaboration with organised crime groups or individual hackers) conduct industrial espionage and/or sabotage. As above, corporations can threaten human rights by collecting and analysing large amounts of personal data and, in some cases, by sharing this data with governments and other private actors.
Hackers	It was once common for hackers to crack into networks for the thrill of the challenge or for bragging rights in the hacker community, although motivations are now far more commonly criminal in nature. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the internet and launch them against victim sites. Thus, attack tools have become more sophisticated and easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on web pages or email servers. Hacktivists seek to disrupt, deface, or destroy web sites in order to achieve political goals.
Disgruntled insiders	Disgruntled insiders are a major threat given that their often detailed knowledge of a victim system can allow them to gain unrestricted access. Insiders may be motivated to cause damage to the system or to steal sensitive data. The US Federal Bureau of Investigations (FBI) reports that attacks by insiders may be twice as likely as those from outsiders.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructure, threaten national security, cause mass casualties, weaken economies, and damage public morale and confidence. While many terrorist groups may currently lack advanced capacity for cyber attacks, there is no guarantee that they will not develop such capabilities in the future (or even purchase them from organised crime groups).
Botnet operators	Botnet operators are hackers who take over large numbers of computers, which are then used to coordinate attacks and to distribute phishing schemes, spam and malware attacks. The services of these networks are sometimes made available in underground markets.
Phishers	Phishers are individuals or small groups who use fraud in an attempt to steal identities or information for monetary gain. Phishers often use spam and spyware/malware to accomplish their objectives.
Spammers	Spammers are individuals or organisations, who distribute unsolicited e-mail (often with hidden or false information) in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organisations.
Spyware and malware authors	Individuals or organisations with malicious intent carry out attacks against users by producing and distributing spyware and malware.
Paedophiles	Paedophiles increasingly use the internet to share child pornography (via email, specialised file-sharing sites, and P2P software) and to recruit victims (often using social networking sites or chatrooms).

[8] adapted from United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk (Washington DC: US GAO, 2009); William A. Wulf and Anita K. Jones, "Reflections on Cybersecurity," *Science* 326 (13 November 2009): 943-4; See Martin Charles Golumbic, *Fighting Terror Online: The Convergence of Security, Technology, and the Law* (New York: Springer, 2007).

Table 2. Categories of Cyber Threats

Category	Sub-category	Examples
Integrity Cyber attacks may use hacking techniques to modify, destroy or otherwise compromise the integrity of data.	Propaganda/disinformation	Modification or manipulation of data or introduction of contradictory data to influence a political or business outcome or destabilise a foreign regime
	Intimidation	Attacks on websites to coerce their owners (both public or private) into removing or modifying content, or pursuing some other course
	Destruction	Permanent destruction of data to hurt competitors or attack foreign governments. This may, for example, form a part of wider conflict.
Availability Denial of service attacks by botnets, for example, may be used to prevent users from accessing data that would otherwise be available to them.	External information	Denial of service, etc. attacks on government or private services available to the public, for example, media outlets, government information sites, etc.
	Internal information	Attacks on private or governmental intranets, for example, emergency services networks, energy and transport control infrastructure, e-banking sites, company email, command and control systems, etc.
Confidentiality Cyber attacks may target various types of confidential information, often for criminal gain.	Espionage	Firms seeking information on their competitors; states involved in spying activities (against both foreign states and individuals)
	Personal data theft	Phishing attacks (or similar) aimed at tricking users into revealing personal data, such as bank account numbers; viruses that record and upload such data from a user's machine
	Identity theft	Trojan horses, and so forth, used to steal identity information that is then used in the commission of crimes
	Data mining	Open source techniques employed to discover, for example, personal information from publicly available data
	Fraud	Often delivered via spam email, fraud includes the popular Nigerian "419" or advanced fee fraud, as well as attempts to convince recipients to buy a range of fraudulent goods or services

Table 3. Responders to Cyber Threats

Type	Example	Role		
		Policy	Response	Enforcement
International and Regional Organisations	APEC-TEL, European Network and information Security Agency (ENISA), NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), ASEAN, OECD, OAS Computer Security Incident Response Teams (CSIRT), Internet Governance Forum (IGF), International Telecommunications Union (ITU), Internet Society (ISOC), Internet Corporation for Assigned Names and Numbers (ICANN), Meridian CIIP, G8 Lyon Group, Subgroup on High-Tech Crime, UN, CoE	X	X (ICANN, Meridian CIIP)	X (G8 Lyon Group, Subgroup on High-Tech Crime)
NGOs	Human rights organisations (such as the American Civil Liberties Union, Human Rights Watch, Amnesty International, Reporters Without Borders, the OpenNet Initiative), foundations (such as the World Wide Web Foundation, Shadowserver Foundation), think tanks (such as CSIS, RAND), among many others	X		
Industry Bodies	Anti-Phishing Working Group (APWG), Domain Name System Operations Analysis and Research Center (DNS-OARC), Messaging Anti-Abuse Working Group (MAAWG), Industry Consortium for Advancement of Security on the Internet (ICASI), Infosec Research Council Science and Technology Study Group on malicious code (ISTSG), Internet Engineering Task Force (IETF), Institute of Electrical and Electronics Engineers (IEEE), transport related bodies (especially airport security/air traffic control), other industry bodies related to critical infrastructure	X (APWG)	X	
States	Ministries of Interior, Foreign Affairs, Transport, and Finance, Intelligence Services, Police Departments (particularly dedicated cyber security units and organised crime squads), Justice Ministries, Computer Emergency Readiness Teams (CERTs), operations security offices, specialised offices of cyber security	X	X	X
Private Sector	Specialised internet security firms, software developers, hardware manufacturers, online payment providers, email servers, online content hosts, banks and financial sector actors, online commerce actors		X	
Individuals	Individual PC owners and users		X	

2. Challenges to Democratic Governance

2.1 Oversight

When faced with both traditional and non-traditional security challenges, states, acting alone, are poorly equipped. Ad hoc security governance networks and, in particular, public private cooperation, has increasingly been the response. It may be tempting to call this process "privatisation" but that would be, as Alyson Bailes argues, to miss the nuances and complexities of a situation in which functions are delegated or shared on a case-by-case basis without the "full transfer or property […] that might occur in industrial 'privatization'."[9] The term "governance network" is more appropriate to the case of cyber security given that the delegation or transfer of responsibility is occurring in two directions. As well as states *reaching down* to firms, companies are also *reaching up* to the state. An example of this is the recent cooperation agreement between Google and the US National Security Agency (NSA) (discussed in more detail below), apparently to help the firm secure its network after a recent attack by Chinese hackers.

Such networks involve cooperation between governments, the private sector, non-governmental and international organisations and enable actors to take advantage of geographical, technological, and knowledge resources they would be unable to muster alone. This emergence of new governance networks poses both theoretical and practical challenges that have, thus far, been massively under-examined.

At the theoretical level, there are gaps in our understanding of complex governance networks. At the practical level, there are, as yet, unanswered questions about the transparency, oversight, accountability and cost (broadly defined) of new governance networks, as well as about ways in which, on the positive side, they can contribute to improved security.

These gaps and problems are particularly acute with regards to public private cooperation. Such cooperation is, by its very nature, often opaque and the activities of a network's constituent parts are often complex and hidden from the gaze of oversight bodies and institutions of democratic governance. In addition, as Bailes points out:

> the balance of *control* in the public-private relationship is shifting in the realm of security […] there are few, if any, instances in which government nowadays can simply force businesses to do what it wants; and even the more obvious methods of indirect control—ranging from national and international legal regulation through to 'fixing' the play of economic incentives—

[9] Alyson Bailes, "Private Sector, Public Security," in *Private Actors and Security Governance*, ed. Alan Bryden and Marina Caparini (Berlin: Lit Verlag, 2006), 42.

> are becoming trickier to apply in an environment increasingly shaped by non-traditional, non-state, multinational or trans-national forces and actors.[10]

The use of private military and security companies has clearly garnered the most attention in this regard. However, cyber security offers us another, no less pertinent, illustration of this problematique. A number of factors exacerbate the oversight challenges presented by cyber security and related public private cooperation. Below is a list of these challenges, followed by some examples from state practice in the UK, US and Australia.

First, oversight challenges are exacerbated by *network complexity*. As is illustrated below, a large and diverse number of state, private, international and other non-state actors are involved in cyber security. Similarly, a huge diversity of actors participate in what we might broadly term cyber attacks. Network complexity makes it difficult for oversight bodies, such as parliamentary committees (with often limited capacity), to keep track of relevant actors, to gain knowledge of their existence and activities or even to acquire a legal mandate to do so.

Second, oversight challenges are exacerbated by *technical complexity*. Because of the highly technical nature of cyber security challenges and responses, oversight bodies often lack the required expertise to understand and adequately oversee them. Public private cooperation exacerbates the problem by creating a divide between the highly paid and sophisticated technical experts involved in implementing a directive and the (often) poorly paid and less well informed government actors charged with their oversight.

Third, oversight challenges are exacerbated by *legal complexity*. Cyber security poses complex legal questions related (among others) to the right to privacy and freedom of expression. This complexity is then magnified by public private cooperation and associated legal questions regarding responsibility and control.

Fourth, oversight challenges are exacerbated by the *heterogeneity of actors* involved. In most instances, oversight institutions are organised along agency or functional lines. For example, a parliamentary committee may oversee intelligence services and activities, the armed forces, or justice. The public private cooperation involved in cyber security, however, cut across agency boundaries and thus across areas of oversight mandate. The result is a large number of areas in which there is no or inadequate oversight.

Fifth, oversight challenges are exacerbated by *mandate perceptions*. In general, government oversight bodies are concerned with the government agencies over which they have direct responsibility. This leaves the private partners of such agencies out

[10] Bailes, "Private Sector, Public Security," 42.

of the reach of oversight, even in cases where they are directly funded by, or work in close collaboration with such agencies.

Sixth, oversight challenges are exacerbated by the *breaking of principal/agent bonds*. The actions of every government agent are connected in a chain of responsibility from principal to agent. For example, a Paris police officer is linked via his or her superiors to the *prevote* (the senior officer in the force), to the prefect (the politically appointed head of the force) and, ultimately, to the interior ministry and the executive. There is thus a link of responsibility and oversight between instruments of democratic governance (such as the parliament) and individuals or agencies carrying out government directives. These links are severed by the introduction of private actors and the creation of public private cooperation mechanisms. While a publicly contracted IT firm may seem to act as a simple agent of the state (the principal), the relationship is generally much more complex and clouded by numerous information asymmetries that reduce transparency and prevent oversight mechanisms from operating effectively.

Because online security is, in many states, a relatively new issue for security actors, democratic oversight, in the form of ombudsmen, parliamentary committees and other specialised bodies, has been slow to catch up. In the UK, for example, oversight of government cyber security efforts is by interdepartmental oversight boards, the cabinet committee for national security, international relations and development and its sub-committee on protective security and resilience. By considering the issue alongside more traditional defence questions, the effectiveness of oversight in the UK may be vulnerable to the problems of *technical complexity, mandate perceptions*, and *legal complexity* that were discussed above.

Similarly, in Australia, the government's cyber security activities are overseen by existing bodies and committees, such as (where intelligence actors are concerned) the Inspector-General of Intelligence and Security and the Parliamentary Joint Committee on Intelligence and Security. This may leave oversight susceptible to problems related to *mandate perceptions* and to the *heterogeneity of actors* that were, again, discussed above.

In the US, the situation is somewhat better, although oversight gaps still remain. The executive has appointed a deputy for civil liberties for the Civil Liberties and Privacy Office of the Office of the Director of National Intelligence, whose role will be to oversee the privacy aspects of government cyber security policy. However, at the congressional level, jurisdiction is shared by at least four authorising committees and a similar number of appropriations sub-committees. Each committee may have a different perspective on the problem, and may try to balance the issues towards their own equities. As with many complex issues involving a *heterogeneity of actors,* fragmentary oversight may hinder efforts at a uniform approach to the problem. To take a recent example, Google and the NSA have recently joined forces as a result of large-scale attacks on the company, said to have come from China. Reports in the

Washington Post stated that the alliance was designed in such as way as "to allow the two organizations to share critical information without violating Google's policies or laws that protect the privacy of Americans' online communications."[11] However, it is unclear to what extent this assurance is verifiable by any kind of extant democratic oversight mechanism or, indeed, how much protection is being offered to foreign individuals.

2.2 Implications for Human Rights Protection

The pace with which network security concerns are outstripping the ability of oversight and regulatory bodies to hold them accountable is particularly worrying when one considers the implications for the rights to privacy and to freedom of expression and of association.

A key part of cyber security strategy among governments, individuals and private industry is the use of firewalls. Essentially, a firewall marks the boundary between two or more networks and regulates traffic between them according to a set of rules or *policy* of varying complexity and sophistication.

At a basic commercial level, firewalls involve public private cooperation because, as described above, private firms commonly develop the hardware and software that they require to run. This relationship is only set to expand as governments worldwide seek to roll out many of the tools that currently protect highly classified networks to a much wider array of government agencies.[12]

At a more sophisticated level, however, public and private actors are increasingly linked by complex regulatory frameworks, particularly related to the electronic protection of critical infrastructure. Given the diversity of actors who own or otherwise control critical infrastructures (including power stations, hospitals, airports, and so forth), there are clearly limits to an approach that only protects government networks. However, while there has been talk of constructing "a firewall for all Americans on the net",[13] it seems increasingly evident that a wall-building arms race is ultimately fruitless. This is particularly the case given that (as in the example immediately above) such defences are only national in scope. As Pavan Duggal, an Indian cyber law expert, rightly suggests, national legislation is "of limited use in protecting users of a borderless communications tool."[14]

[11] Ellen Nakashima, "FBI Director Warns of 'Rapidly Expanding' Cyberterrorism Threat," *The Washington Post*, 4 March 2010.

[12] Ryan Singel, "Report: Government's Cyber Security Plan is Riddled With New Spying Programs," *Wired*, 15 May 2008, Threat Level.

[13] Ibid.

[14] Pavan Duggal cited in William Maclean, "Cyber Evil Will Thrive Without Global Rules – Good Luck With That," *Wired,* 22 February 2010, Epicenter.

Table 4. Internet Censorship[15]

According to the OpenNet Initiative, states can be divided into the following three classes relating to their level of internet censorship	
Pervasive	Burma (Myanmar), China, Cuba, Egypt, Iran, North Korea, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan, Vietnam
Substantial	Australia, Bahrain, South Korea, United Arab Emirates, Yemen
Nominal	Belarus, Belgium, Brazil, Canada, Chile, Croatia, Czech Republic, Denmark, Estonia, Fiji, Finland, France, Germany, Ghana, Ireland, India, Israel, Italy, Jordan, Malaysia, Morocco, Netherlands, New Zealand, Norway, Pakistan, Poland, Russia, Singapore, Slovenia, Sweden, Thailand, Turkey United Kingdom, United States

Attempts to build national firewalls (or similar systems for controlling international data traffic) have often met fierce opposition from private actors and their cooperation with governments in this area is, more often than not, coerced. In Australia, for example, where the current government has proposed legislation that would require ISPs to block certain websites and types of content, proposals have met with strong opposition from both industry and civil society. Google, for example, commented that the proposed legislation is "heavy handed and can raise genuine questions about restrictions on access to information" before going on to argue that, while "this type of content may be unpleasant and unpalatable [...] government should not have the right to block information which can inform debate of controversial issues."[16]

In addition, the dispersal of responsibility that often characterises public private cooperation, for example, has direct consequences for the protection of human rights. When states and private industry cooperate in the pursuit of law enforcement goals, it becomes much harder to attribute responsibility when, for example, human rights violations are found to have taken place. In a recent and long running case in the US, it has been revealed that AT&T, a US telecommunications giant, funnelled enormous quantities of communications data (emails, telephone calls, and so forth) to the National Security Agency (NSA) without a warrant. In subsequent legal action, it has been difficult to know whether to name telecommunications firms or the government as the defendant as neither is taking any responsibility.[17] See Box 1.

Of further concern is the fact that there is a fundamental tension between protection of privacy rights and improved identification and authentication of users. This feature of cyber security—the difficulty and technical expertise required to identify online "bad guys"—has led directly to a secondary threat: the fact that states and firms are collecting and analysing vast amounts of personal and private data in the pursuit of their own (and their client's) security, often without adequate democratic oversight. Indeed, Lt. General Keith Alexander, who has been nominated to lead the

[15] OpenNet Initiative, "Country Profiles," OpenNet, http://opennet.net/research/profiles

[16] Google, "Our views on Mandatory ISP Filtering," *Official Google Australia Blog: News and notes from Google Down Under*, 16 December 2009.

[17] David Kravets, "Courts, Congress Shun Addressing Legality of Warrantless Eavesdropping," *Wired*, 29 January 2010, Threat Level.

new US Cyber Command, recently told the Senate Armed Services Committee that the impact on privacy of new IT security measures was "classified."[18]

Various efforts and proposals have been made with regards to the fast identification of hackers and cyber criminals. In one example, the US Defence Advanced Research Projects Agency (DARPA) has tabled plans for what it calls a "cyber genome" project that would make documents or codes traceable to their origins—a kind of modern day equivalent of WWII radio operators becoming identifiable, even over encrypted channels, by the distinctive "fist" with which they operated their Morse keys.[19] Less extreme plans involve legislation, proposed in many jurisdictions, which would force ISPs to retain user data—including which subscriber account was assigned a dynamic IP address at a particular time—for several years.

Box 1. Telecoms Immunity[20]

In June 2008, the US House of Representatives passed a law which granted immunity from prosecution to a number of US telecoms companies, including AT&T and Verizon. This immunity protects them from more than forty lawsuits arising from their role in government programmes, established by the Bush administration, which involved the warrantless surveillance of email and internet traffic. The lawsuits allege that the firms in question violated privacy laws and enabled spying without a warrant.

The legislation and the actions of US telecoms firms that led to it raise important questions about the accountability of private actors in public private cooperation networks related to cyber security. As Democratic senator Patrick Leahy, chairman of the Senate Judiciary Committee, argued: "My interest is not in harming telecommunications carriers. I would have supported indemnification by the government or substitution of the government for them in these lawsuits […] But for me, there must be accountability."[5]

For example, the European Court of Human Rights found, in the 2008 case of KU v. Finland, that enough legislation exists to support member states authorities' request of data from ISPs when it is required in the course of a criminal investigation.[21] The court based its finding on a number of examples of European law and practice, including the European Committee of Ministers' Recommendation No. R (95) 13 concerning criminal procedure law for information technology crimes and the European Convention on Cybercrime, both of which impose obligations on service providers to provide information to identify users when ordered by competent investigating authority.[22] The court also made reference to EU Directive 2002/58/EC, article 5 of which states that: "[M]ember States shall ensure that the following categories of data are retained under this Directive: (a) data necessary to trace and identify the source of a communication [...] (2) concerning Internet access, Internet e-mail and Internet telephony [...] (iii) the name and address of the subscriber or registered user to whom

[18] Steven Aftergood, "Privacy Impact of Internet Security is Classified, NSA Says," *Secrecy News: Secrecy News from the FAS Project on Government Secrecy*, 21 April 2010.

[19] Noah Shachtman, "'Don't Be Evil,' Meet 'Spy on Everyone': How the NSA Deal Could Kill Google," *Wired*, 4 February 2010, Danger Room.

[20] Elana Schor, "Telecoms Granted Immunity in US Wiretapping Probe," The Guardian, 20 June 2008.

[21] KU v. Finland [2008] ECHR 2872/02)

[22] Ibid.

an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication."[23]

However, these trends face pressure from the opposite direction. In 2008, the EU's own Article 29 Data Protection Working Party, for example, put Google under enormous pressure over its data retention policies. EU Justice Commissioner Jacques Barrot told Reuters that a decision by the company to make IP and cookie data anonymous after 9 months (instead of the previous 18) was "a good step in the right direction" although still not enough to protect user's privacy.

Furthermore, the global nature of the networks involved substantially complicates the issue. Here, effective cyber security faces the same barriers as other international cooperation efforts. With the added complexity of private sector involvement (see Box 2.). If a website hosting malicious content has, for example, a .ch (Swiss) address, yet is owned in Russia and hosted in the Netherlands, who then is responsible and which legal system applies? Even finding out this information in the first place—who is behind an IP address—requires the cooperation of private sector actors, many of whom either do not hold on to the relevant data, or are reluctant to share it for fear of driving away customers.

This problem is compounded by the fact that many states have no (or only very limited) legislation on the issue. In many of these jurisdictions, even if there were political will, there is none of the requisite technical capacity to design or implement such legislation, even if it did exist. Lack of legislation and capacity means that criminals can access the Internet anonymously from an impoverished state (via, for example, an unregistered SIM card) and commit crimes abroad with impunity.[24] Such states are in danger of becoming what Datuk Mohammed Noor Amin, chairman of the UN-affiliated International Multilateral Partnership Against Cyber Threats, has called "cyber failed states."[25] Given the high costs of online security (estimated at between 3 and 10 percent of IT budgets) it is unclear how quickly such states will be able to muster the resources required.

There is a need for a common strategy and shared norms at the international level. However, efforts to promote international cooperation will inevitably come up against the challenge of balancing anonymity, privacy and openness with efforts to share information and better track criminals. The kind of tool DARPA describes would, for example, be highly useful to repressive regimes looking to stamp out political dissent. Even the retention of user data by ISPs has been called "invasive, risky, unnecessary, and likely to be ineffective" by the Centre for Democracy and Technology.[26] Furthermore, in a large number of states, insufficient oversight exists to

[23] cited in KU v. Finland [2008] ECHR 2872/02
[24] Maclean, "Cyber Evil Will Thrive Without Global Rules – Good Luck With That"
[25] Noor Amin cited in Maclean "Cyber Evil Will Thrive Without Global Rules – Good Luck With That"
[26] Julian Sanchez, "New Bill Would Force ISPs to Retain User Data for Two years," *Ars Technica,* 19 February 2009.

prevent possible government abuse of such requests for data on identity and use, for many of the reasons cited in the preceding section.

As the Centre for Strategic and International Studies (CSIS) suggests in a recent report, "while anonymity and weak authentication of identity create some of the greatest security challenges in cyberspace, they also serve to protect those who, for example, want to engage in unpopular speech."[27] The report suggests a solution based on ranking online activities by risk, with activities such as online shopping at one end of the spectrum (low risk) and accessing the control systems for critical infrastructure at the other (high risk). Individuals would then be free to use low levels of authentication for some online actions but be forced to provide robust credentials when engaging in higher risk activities.[28]

Box 2. International Cooperation and the Mariposa Botnet

In May 2009, Defence Intelligence, a private Canadian security firm, detected a giant botnet, codename Mariposa, which had infected more than 13 million machines in more than 190 countries. Among the infected machines were computers in major banks and in more than half of the world's 1,000 largest companies.

The botnet was being used by its Spanish owners to steal vast amounts of personal information, particularly banking and credit card details. Parts of the botnet were also being rented to various organised crime groups.

After its discovery in May, Defence Intelligence collaborated (among others) with a Spanish firm, Panda Security, as well as with the US FBI and the Spanish police to uncover the owners of the network and, eventually, to arrest them and shut it down.

2.3 Deterrence and Responding to Cyber War

One consequence of the problem described above—that the origin of the threat is hard to identify—is that traditional deterrence and response policies have been undermined. Because it is extremely difficult to pinpoint the origin of attacks, it is hard to deter further damage by threatening retaliation.[29]

Scholars of cyber war have thus concluded that there is little or no defensive benefit to be gained from having great offensive capabilities. James A. Lewis, of the Centre for Strategic and International Studies, notes that, "the US is widely recognised to have pre-eminent offensive cyber capabilities but it obtains little or no deterrent effect from this."[30] It is, of course, possible that credible deterrents will yet be identified but, for the moment, recent cyber battles have outpaced efforts to find one. As Joseph Nye remarked in the New York Times, "we are now in the phase that we found ourselves in during the early 1950s, after the Soviets got the bomb […] it won't have the same shape as nuclear deterrence, but […] we can create some high costs for attackers."[31]

[27] Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington DC: CSIS, 2008).
[28] Ibid.
[29] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Washington DC: RAND, 2009).
[30] Markoff, Sanger and Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent"
[31] quoted in Markoff, Sanger and Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent"

A further problem is that, even if an attacker is properly identified, it may be difficult to adequately respond. In part, this is due to the extreme difficulty of differentiating reliably between vandalism, commercial theft, or state-sponsored cyber-war.[32] And, just as cyber war has blurred distinctions between categories of attacker, it has also blurred civil and military categories of target. Thus, a cyber attack can effectively cripple a country by, for example, attacking its financial industry, without ever targeting a military or government asset.[33]

This fact raises serious problems for those seeking to respond. The UN Charter, in article 2(4), states that: "All 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." This principle, which now forms part of customary international law, bans the use of force in all but two carefully defined situations: first, the Security Council may authorize collective action to maintain or enforce international peace and security and, second, states may act in "individual or collective self-defence if an armed attack occurs against a state." Speaking about the Estonian cyber war (see Box 3.), Jaak Aaviksoo, the then Estonian defence minister, remarked:

> At present, NATO does not define cyber-attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defence, will not automatically be extended to the attacked country […] Not a single NATO defence minister would define a cyber-attack as a clear military action at present. However, this matter needs to be resolved in the near future.[34]

Meanwhile, debate continues about what states are able to credibly threaten—diplomatic demarche, formal protest, economic retaliation, criminal prosecution, pre-emptive attack, or military strike.[35] The creation of a NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, with a mandate to improve cyber defence, suggests that the alliance expects the Estonian cyber war to be only the beginning. Indeed, the centre's website argues that: "Modern militaries are preparing to use cyberspace as a parallel battleground in future conflicts […] Even when a purely network-based attack is unlikely, cyber attacks employed in concert with conventional weapons will become the standard operating procedure in future conflicts."[36] And while many states rush to gain the technical capabilities required for participation in this "revolution in military affairs", relevant norms and structures regarding transparency, accountability and oversight, struggle to keep pace.

[32] Markoff, Sanger and Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent"

[33] Franklin D. Kramer, Stuart H. Starr and Larry Wentz, eds., *Cyberpower and National Security* (Washington DC: Center for Technology and National Security Policy, National Defence University, 2009).

[34] Jaak Aaviksoo quoted in Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, 17 May 2007.

[35] Jeffrey Carr, "Responding to International Cyber Attacks as Acts of War," in *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol CA: O'Reilly Media, 2010).

[36] Cooperative Cyber Defence Centre of Excellence, "General Trends," CCDCOE, http://www.ccdcoe.org/8.html

Box 3. The Estonian "Cyber war"[37]

As one of the most electronically advanced countries in the world, the Estonian government has increasingly shifted its operations to the virtual domain. Cabinet-level meetings are conducted online and Estonian citizens can cast their votes in national elections via their computers.7 In 2007, Estonia was ranked 23rd in e-readiness ratings. Almost 61 percent of the population enjoys online access to their bank accounts, and 95 percent of banking transactions are electronic.

This connectivity, however, is also a vulnerability. In April 2007, the Estonian Parliament, ministries, banks and media institutions were hit by a series of coordinated distributed denial of service (DDoS) attacks. The relocation of the Bronze Soldier of Tallinn, a Soviet-era war memorial, sparked protests and riots among Estonia's Russian minority. These protests were then followed by distributed denial of service (DDoS) attacks to temporarily prevent access to (and in some cases deface) a number of key Estonian websites. A call for action, complete with specific instructions on how to participate in the DDoS attacks, quickly spread through Russian online chat rooms. As a result, the websites of the Ministries of Foreign Affairs and Justice had to shut down, while Prime Minister Andrus Ansip's Reform Party website was defaced. The attack also briefly disabled the national emergency telephone number. Intermittent cyber attacks on national government websites, including the State Chancellery and Federal Electoral Committee, continued well into the middle of May 2007.

Assessments regarding the severity and implications of the attack vary widely, complicated by the fact that some evidence points to involvement by Russians in coordinating or otherwise supporting the attack. Part of the problem, as with any internet crime, was that even though the root of the attack was widely recognised, there was no recourse possible. Despite some more outlandish claims made at the time, however, it is now generally accepted that the attacks were more a "cyber dispute" than a "cyber war" and—while problematic for a small state like Estonia—not particularly sophisticated from a technical standpoint, or especially indicative of what the future might hold. Indeed, Estonia's computer emergency response team (CERT)—as in most other states, a body that coordinates public and private actors to deal with online threats – responded quickly and competently to the attack, using packet filtering and other well-established and successful techniques.

Many have pointed to the events in Estonia as merely a precursor of much more serious and devastating future battles. However, the danger, other commentators argue, is that by overstating the impact of cases such as Estonia, we may drift too far in the other direction, towards a more closed internet, in which the identity of attackers is perhaps easier to ascertain, but in which fundamental freedoms—such as the rights to privacy and freedom of expression—are also less assured. In particular, critics posit that proposals to, for example, "re-engineer the Internet to make attribution, geo-location, intelligence analysis and impact assessment more manageable", as Michael McConnell, the former director of US national intelligence, suggests we should, will also lead to unwanted government control and surveillance over what we write in our emails, type into a search engine, or download from a website.

A number of further issues hinder democratic governance with regards to responses to cyber war. The first of these is a dispersal of responsibility. In short, it is often extremely difficult to work out who is in charge of a relevant area because of the huge convergence of many previously distinct sectors. There is thus a need to bridge previously distinct roles, ministries, and threat-response mechanisms. This is particularly the case with regards to the increasingly artificial distinction between national security and other government networks and different roles and responsibilities. The same is true in the legal domain, where a patchwork of laws exists that evolved to cover what were originally very distinct fields of activity. More

[37] Some of the material in this box was kindly contributed by Mr. Fred Schreier. See also Cyrus Farivar, "Cyberwar I. What the Attacks on Estonia Have Taught Us About Online Combat," *Slate*, 22 May 2007; Johnny Ryan, "iWar: A New Threat, Its Convenience – and Our Increasing Vulnerability," *NATO Review*, Winter 2007; Shaun Waterman, "Who Cyber Smacked Estonia?" *United Press*, 11 June 2007; Kevin Poulsen, "'Cyberwar' and Estonia's Panic Attack," *Wired*, 22 August 2007, Threat Level; Singel, "Report: Government's Cyber Security Plan is Riddled With New Spying Programs"

than ever, there is a need for clearly identified roles and responsibilities, both within and between public and private actors.[38]

Secondly, actors are often highly reluctant to share information, something that is of growing concern for policymakers given the large number of players who have time-critical information. To take just one example, firms have incentives to keep security measures secret until they are deployed, in order to protect valuable proprietary information. The consequence of which is that the flaws in such measures only become apparent after they have been deployed.[39] Unless they are the explicit target, governments also often have no way of knowing if an attack has taken place. Referring to the recent attack on Google, for example, one senior intelligence official said, "unless Google had told us about the attack on it and other companies, we probably never would have seen it. When you think about that, it's really scary."[40] A parallel problem, of course, is that governments may be unaware that people or firms may be using their territory to launch attacks.

Possible solutions to this problem include proposed "cyber incident thresholds" after which reporting becomes mandatory, although given that there are a huge number of low level events that together have a large impact, it is unclear how effective this would be overall. In a similar vein, the United Kingdom has developed a system to encourage information sharing in which data ownership never changes hands. Instead, it is passed to vetted "information security providers" who act as a nexus for combining data rather than the government.[41] Trust and transparency are key issues for private actors, many of whom are fearful, both of losing market share should they become forced to divulge too much information (on clients, and so forth) to governments, as well as of malicious attacks by hackers. There are also scores of unresolved legal issues related to aggregation of authorities, what authorities are available for the government to protect privately owned critical infrastructure, placement of monitoring software, automated attack detection and warning sensors, data sharing with third parties and liability protection for the private sector.

Others have proposed the creation of powerful state-level entities that combine information from various actors (such as local cyber security centres) with the goal of developing a comprehensive picture of cyber threats and network status, as well as of supporting coordinated incident response. At the government level, coordination requires cooperation between law enforcement, intelligence, counter-intelligence, and the military on all remote intrusions, insider operations and supply chain vulnerabilities,[42] as well as planning, detection, prevention, and incident response. These need to be integrated into a comprehensive framework, particularly with regards to incident response and end-to-end system design—something that no one is currently responsible for.

[38] White House, *Cyberspace Policy Review*

[39] Jim Giles, "Benevolent Hackers Poke Holes in E-Banking," *New Scientist*, 29 January 2010.

[40] Markoff, Sanger and Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent"

[41] White House, *Cyberspace Policy Review*

[42] Ibid.

Box 4. The Georgian Conflict[43]

The cyber attack on Georgia was the first online assault carried out in conjunction with a military offensive. Small-scale DDoS attacks began in June, almost two months before the five-day war between Russia and Georgia over Georgia's breakaway region of South Ossetia.

On the 20th of July, the Shadowserver Foundation, an Internet watchdog group, registered multiple DDoS attacks targeting the official website of Georgian President Mikhail Saakashvili. The attack, which shut down the presidential website for more than 24 hours, was directed by a server in the US, a fact which underlines the borderless nature of the threat.

The DDoS attacks against Georgia's nascent internet infrastructure reached an alarming level on the 8th of August, the first day of the war. On that day, Shadowserver detected the first attack by six different botnets against Georgian government and media websites. As the conflict escalated, so did the online attacks, with Russian hacktivists shutting down and defacing the websites of the President, the Georgian Parliament, the Ministries of Defense and Foreign Affairs, the National Bank of Georgia, and two online news agencies.

The Georgian government reacted swiftly and creatively. With Google's permission, the websites of the Ministry of Foreign Affairs and Civil.ge were temporarily transferred to the Blogspot domain where they were better protected against attack. On the 9th of August, the Atlanta-based Internet service provider Tulip Systems Inc., owned by the Georgian-born Nino Doijashvili, began to host the President's website. In a gesture of solidarity, the President of the Republic of Poland, Lech Kaczynski, graciously provided space on his website for the official press releases of the Georgian government. The Estonian government provided substantial assistance by accommodating the website of the Ministry of Foreign Affairs and dispatching two information security specialists to bolster Georgian cyber defences.

According to Belarusian digital activism expert Evgeny Morozov, coordination of the attacks was largely carried out by an online hacker forum StopGeorgia.ru. Set up hours after the Russian armed forces invaded South Ossetia, this forum featured a constantly updated list of target websites and encouraged visitors to download a free software programme, which allowed them to participate instantly in the attacks.

There is also evidence to suggest that simpler but equally effective SQL injection attacks were also used. These attacks overwhelm the targeted database with millions of junk queries, thereby rendering the corresponding server inoperable. From a hacker's perspective, SQL attacks provide two main advantages. First, when used in combination with traditional DDoS attacks, they are extremely difficult to detect. Second, SQL injection attacks require far fewer computers to achieve the same objectives as DDoS attacks, which cannot be sustained effectively without botnets.

In the end, the cyber attacks inflicted little damage because much of Georgia's economy and critical infrastructure are still not integrated into the Internet. Nonetheless, the campaign waged by nationalist hacktivists, spurred into action with the help of Russian online hacker forums, effectively disrupted the dissemination of information by the Georgian government at a crucial stage in the conflict.

[43] The material in this box was kindly contributed by Mr. Fred Schreier

Conclusions

A number of things are clear from the discussion above. First, combating online threats requires states to look beyond the whole of government paradigm and embrace instead an approach that places effective and efficient public private cooperation at its heart. To take just one example, law enforcement agencies are hampered by a dispersal of effort and responsibility, the fact that the tools required to respond are often in the hands of others (defence or intelligence agencies, for example), and public private cooperation networks are difficult to formally establish or make work. This last point is particularly the case given that both sides may wish to keep crucial information secret – all the more so when the firms involved are international or foreign owned. These partnerships must involve, not only the private actors involved in so-called critical sectors, but also specialised internet security firms, software developers, hardware manufacturers, online payment providers, email servers, online content hosts, banks and financial sector actors, online commerce actors and private individuals.

Given that online threats are commonly international in nature, transnational partnerships may also be necessary. However, problems here are even more pronounced than at the national level and joint policies and approaches among regional and international actors are still underdeveloped. Compounding the problem is the existence of a profound capability gap (in terms of equipment, expertise and, crucially, institutions and oversight) between different states, gaps that are only likely to widen.

Second, this paper has made clear that the public-private cooperation that are required for comprehensive and effective cyber security raise difficult and, as yet, unresolved questions related to oversight and accountability and, in particular, to fundamental rights such as the right to privacy and to expression and association. As was pointed out above, the challenge of online security parallels to tension (apparent in many other security domains) between state and human security, with the added dimension of powerful private actors, with their own motives and priorities. A lack of transparency compounds the myriad difficulties faced by relevant oversight bodies, where they exist at all.

Third, the possibility of cyber war – alongside questions about how big its impact on war fighting will ultimately be – raises new questions about state response and about the democratic oversight and legal challenges that any response must face. At what threshold does an attack become a cyber war, and what tools can be used in response are as yet unanswered questions, questions that pose very new questions for SSR and SSG.

This paper offers but a brief overview of these issues. In consequence, and in common with all the papers in the Horizon 2015 series, it seeks to raise more questions than it answers. Some of these questions include:

- How can the evolution and identification of cyber threats be monitored (and the available responses improved) while still maintaining anonymity online?
- How can the capacity and mandate of relevant oversight structures be improved to deal with this cross-cutting and highly technical issue, particularly given the growing involvement and role of intelligence agencies?
- If there is a cyber gap between the US and Europe and a cyber abyss between the OECD and the developing world, how can cyber failed states be prevented and the South's ability be improved to meet the security, regulatory, and technical challenges of online security?
- How can states detect and respond to the emerging threat of cyber war? Clearly, new forms of private public cooperation are needed. But what form should they take, how transparent should they be, and how can they be best subjected to parliamentary and democratic control?
- What is the responsibility of states regarding attacks by groups and individuals operating on their territory?
- How can regulation deal with the international nature of the threat? What international approaches and norms are conceivable and needed? Who should take the lead in this issue?
- What direction for the internet: democratic tool or a major step towards George Orwell's "1984"?
- How to shape, in an open debate, national consensus, strategies, and policy in this area?
- Is cyber war replacing kinetic energy as the core essence of military power? Are we unwittingly witnessing a second wave of the Revolution in Military Affairs? Is the face of battle to be fundamentally changed? If so, what will be the implications for armed forces and the security sector at large? What will be the implications for intelligence services? For law enforcement agencies?
- Is time on our side? Or is technological change outpacing regulatory efforts and the drive for democratic control?

Responses to these and other questions must be the subject of further and detailed analysis.

References

Aftergood, Steven. “Privacy Impact of Internet Security is Classified, NSA Says.” *Secrecy News: Secrecy News from the FAS Project on Government Secrecy*, 21 April 2010.

Arquilla, John and David Ronfeldt, eds. *In Athena’s Camp: Preparing for Conflict in the Information Age.* Washington DC: RAND, 1997.

Bailes, Alyson. “Private Sector, Public Security.” In *Private Actors and Security Governance,* edited by Alan Bryden and Marina Caparini, 41-64. Berlin: Lit Verlag, 2006.

Carr, Jeffrey. “Responding to International Cyber Attacks as Acts of War.” In *Inside Cyber Warfare: Mapping the Cyber Underworld,* 45-74. Sebastopol CA: O’Reilly Media, 2010.

Center for Strategic and International Studies. *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency.* Washington DC: CSIS, 2008.

Cooperative Cyber Defence Centre of Excellence. “General Trends.” CCDCOE. http://www.ccdcoe.org/8.html (accessed 20 April 2010).

Farivar, Cyrus. “Cyberwar I. What the Attacks on Estonia Have Taught Us About Online Combat.” *Slate*, 22 May 2007.

Giles, Jim. “Benevolent Hackers Poke Holes in E-Banking.” *New Scientist,* 29 January 2010.

Google. “Our views on Mandatory ISP Filtering.” *Official Google Australia Blog: News and notes from Google Down Under,* 16 December 2009.

Golumbic, Martin Charles. *Fighting Terror Online: The Convergence of Security, Technology, and the Law.* New York: Springer, 2007.

Kramer, Franklin D., Stuart H. Starr and Larry Wentz, eds. *Cyberpower and National Security.* Washington DC: Center for Technology and National Security Policy, National Defence University, 2009.

Kravets, David. “Courts, Congress Shun Addressing Legality of Warrantless Eavesdropping.” *Wired,* 29 January 2010, Threat Level.

KU v. Finland [2008] ECHR 2872/02)

Libicki, Martin C. *Cyberdeterrence and Cyberwar.* Washington DC: RAND, 2009.

Lloyd’s Emerging Risks Team. *Digital Risks: Views of a Changing Risk Landscape.* London: Lloyds, 2009.

Maclean, William. “Cyber Evil Will Thrive Without Global Rules – Good Luck With That.” *Wired,* 22 February 2010, Epicenter.

Markoff, John, David E. Sanger and Thom Shanker. “In Digital Combat, U.S. Finds No Easy Deterrent.” *New York Times,* 25 January 2010, World section.

Nakashima, Ellen. “FBI Director Warns of ‘Rapidly Expanding’ Cyberterrorism Threat.” *The Washington Post,* 4 March 2010.

OpenNet Initiative. “Country Profiles.” OpenNet. http://opennet.net/research/profiles (accessed 20 April 2010).

Poulsen, Kevin. “‘Cyberwar’ and Estonia’s Panic Attack.” *Wired,* 22 August 2007, Threat Level.

Ryan, Johnny. “iWar: A New Threat, Its Convenience – and Our Increasing Vulnerability.” *NATO Review*, Winter 2007.

Sanchez, Julian. “New Bill Would Force ISPs to Retain User Data for Two years.” *Ars Technica,* 19 February 2009.

Schor, Elana. “Telecoms Granted Immunity in US Wiretapping Probe.” *The Guardian,* 20 June 2008.

Shachtman, Noah. “’Don’t Be Evil,’ Meet ‘Spy on Everyone’: How the NSA Deal Could Kill Google.” *Wired,* 4 February 2010, Danger Room.

Singel, Ryan. “Report: Government’s Cyber Security Plan is Riddled With New Spying Programs.” *Wired*, 15 May 2008, Threat Level.

Traynor, Ian. “Russia Accused of Unleashing Cyberwar to Disable Estonia.” *The Guardian,* 17 May 2007.

United States Government Accountability Office. *Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk.* Washington DC: US GAO, 2009.

Waterman, Shaun. “Who Cyber Smacked Estonia?” *United Press*, 11 June 2007.

White House. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* Washington DC: White House, 2009.

Wood, Jennifer and Benoît Dupont, eds. *Democracy, Society and the Governance of Security.* Cambridge: Cambridge University Press, 2006.

Wulf, William A. and Anita K. Jones. “Reflections on Cybersecurity.” *Science* 326 (13 November 2009): 943-4.

Annex 1.

Critical Infrastructure Protection (CIP), Critical Information Infrastructure Protection (CIIP), and Cyber Security: Overview of Country-Specific Organisational Structures.[44]

- In **Australia**, the Cyber Security Operations Centre is responsible for CIP/CIIP. Launched in 2009 under the government's cyber security strategy and operated by the Defence Signals Directorate (DSD). It is staffed by specialists from the DSD, the Defence Intelligence Organization, the Defence Force, the Federal Police, and the Australian Security Intelligence Organization. The specifics remain secret but the centre advises the government on how best to protect the nation from cyber threats, linking expertise and intelligence in a coordinated response.

- In **Austria**, there is no single authority responsible for CIP/CIIP. All ministries have their own specific security measures to defend against outside attacks and to prevent the unauthorised use of data. Several divisions of the Ministry of Internal Affairs (BMI) deal with CIIP, particularly related to data security and cyber-crime. The head office for public safety at the Federal Crime Police Office operates a reporting centre for child pornography. The Federal Agency for State Protection and Counter-Terrorism (BVT) is responsible for the coordination of personal security and the security of installations. Department II of the Ministry of Defence is responsible for all aspects of information warfare and fulfils its duties in close cooperation with the two intelligence services. One of these, the Abwehramt, has a special Department for Electronic Defence. The Ministry for Traffic, Innovation, and Technology (BMVIT) is responsible for public CIP. It also coordinates the Austrian Security Research Program. In Austria, cyber security is mainly perceived as an issue of data protection, as the Austrian e-government Program, the Official Austrian Data Security Website, or the Pilot Project Citizen Card indicate.

- In **Belgium**, the Ministerial Committee for Security and Intelligence has ultimate responsibility for the development of national information security policy. The Federal Public Service Directorate-General Enforcement and Mediation is the main organisation in charge of implementation of the policy. The Privacy Protection Commission ensures protection of personal data. The Belgian Institute for Postal Services and Telecommunications Breaches is responsible for implementing and ensuring compliance with electronic communications legislation. A national Computer Emergency Response Team (CERT) has yet to be established, although the BELNET network runs a CERT for its constituents in the public and education sectors. In 2008, a whitepaper was published jointly by several academics and private associations with expertise in IT security, proposing the establishment of a cyber security strategy and several measures to improve Belgian information security.

[44] The information in this annex was kindly contributed by Mr. Fred Schreier

- In **Brazil**, public efforts concerning CIIP include: the Information Security Steering Committee, composed of representatives from every ministry; the national policies for ICT under the auspices of the Ministry of Science and Technology, the Ministry of Communications, and the Brazilian Network Information Centre. Brazil has a complex and sophisticated system of institutions involved in developing information security policy. Information security issues lie within the jurisdiction of the Institutional Security Cabinet (GSI), an organ of the presidency with responsibility for coordination of information security. GSI does not handle security issues directly, but works through other related organisations. As for public-private partnerships, Anatel (the federal telecommunications regulatory body), Serpro (the federal data processing service), and CERT.br strive to further and deepen cooperation between the public and the private sector.

- In **Canada**, the Canadian Cyber Incident Response Center (CCIRC) is responsible for monitoring and providing mitigation advice on cyber threats and coordinating the national response to any cyber security incident. Its focus is the protection of national critical infrastructure against cyber incidents. A number of Canadian departments, including the Royal Canadian Mounted Police, the Communications Security Establishment, and the Canadian Security Intelligence Service are involved in responding to cyber-threats. In February 2010, the government announced that a National Cyber-Security Strategy would be forthcoming, marking the third time in less than a decade that the government has said it would produce such a strategy.

- In **Estonia**, the *Cyber Security Strategy* published in 2008 discusses the status quo and defines policies for enhancing cyber security. There is no single central authority responsible for CIIP. Several ministries and their respective subunits are directly involved. The main tasks of CIIP are assigned to the Ministry of Economic Affairs and Communications (MEAC). MEAC plays a leading role with regard to information security and two central agencies for national IT policy are subordinated to it: the Department of State Information Systems (RISO) (which is the central body for overall ICT coordination), and the Estonian Informatics Center (RIA) (which develops and manages data communication services for governmental organisations, is responsible for the technical security of the state's CII, and monitors overall IT security). The Estonian Computer Emergency Team (CERT) is established within the RIA. The Estonian National Communications Board manages and regulates the postal sector as well as the market for electronic communications in Estonia. Other important public agencies that deal with CIIP are located within the Ministry of Internal Affairs and within the Ministry of Defence. These two ministries are responsible for internal security and crisis management. The Computer Protection 2009 project is an important public-private partnership, which aims to improve information security.

- In **Finland**, cyber security is seen as a data security issue and as a matter of economic importance that is closely related to the development of the Finnish information society. There are three major public agencies dealing with CIIP: the Communications Regulatory Authority (FICORA) within the Ministry of Transport and Communications (which promotes the Information Society and handles technical regulation and standardisation); the National Emergency Supply Agency (NESA) (which analyses threats and risks against CII); and the Steering Committee for Data

Security in State Administration (VAHTI) (that develops policy guidelines and practical guides for the security of IT systems). In addition, there are three public-private partnerships in the field of CIIP: The National Emergency Supply Council (NESC), the Ubiquitous Information Society Advisory Board, and the Finnish Information Society Development Centre (TIEKE).

- In **France**, the Secretary-General of National Defence (SGDN), attached to the Prime Minister's Office, bears complete responsibility for organising CIP. In France, cyber security is seen both as a high-tech crime issue and as an issue affecting the development of the information society. L'office central de lutte contre la criminalité liée aux technologies de l'information et des communications (OCLCTIC), created in May 2000 and part of the Sous-Direction des Affaires Economiques et Financières de la Direction Centrale de la Police Judiciaire, is tasked with investigations of the crime issues. In July 2009, l'Agence nationale de la sécurité des systèmes d'informations (ANSSI) was created within the ministry of defence and is responsible for CIIP and cyber security. Furthermore, there is an Inter-Ministerial Commission for the Security of Information Systems (CISSY). As a public-private partnership, the Strategic Advisory Board on Information Technologies (CSTI) strives to bring together government officials, business and industry executives, and representatives of the R&D community.

- In **Germany**, the National Strategy for Critical Infrastructure Protection (CIP Strategy) summarises the government's aims and objectives and its political-strategic approach. These are included in the *National Plan for Information Infrastructure Protection* (NPSI). The Federal Office of Information Security (the Bundesamt für Sicherheit in der Informationstechnik [BSI]), which is part of the Ministry of the Interior, is the lead authority for cyber security matters. The BSI develops threat assessments, analysis and protection concepts together with the Federal Office for Civil Protection and Disaster Assistance (BBK), the Federal Criminal Police Office (BKA), the Federal Police (BPOL), and the Federal Institute Technical Support Service. For coordination within the ministry and subordinate agencies, a task force for CIP (AG KRITIS) was established. Strategy development and implementation are also coordinated with other federal ministries, especially the Federal Ministry of Economics and Technology, the Federal Chancellery, the Federal Ministry of Justice, the Federal Ministry of Foreign Affairs, the Federal Ministry of Defence, and other relevant agencies, such as the Federal Network Agency. Furthermore, strategic partners from the private sector are consulted.

- In **Hungary**, the government was restructured in 2006. With regard to CIIP and the development of an information society, the most important change was the integration of the Ministry of Informatics and Communications – which was the central body for questions related to ICT – into the Ministry of Economy and Transport and the Prime Minister's Office. The major tasks of CIIP are now allocated to different ministries. As the ministry responsible for the maintenance and development of economic infrastructure, including information infrastructure, the Ministry of Economy and Transport coordinates various CIP and CIIP efforts. Through the Electronic Government Centre, the Prime Minister's Office coordinates efforts regarding e-government as well as other CIIP-related issues. The Ministry of

Defence is responsible for national security, including the security of information, and for protecting state secrets and public data. The duties and responsibilities of the Ministry of Justice and Law Enforcement include crime prevention and data protection, it also controls the Public Administration and Central Electronic Public Services Office, which is the central body for all tasks relating to the provision of e-government services and the management of electronic records and documents. The National Communications Authority (NCA) is an independent regulatory body for communications that supports the development of the communications market and ensures that every citizen has access to affordable and reliable communications services. It is also responsible for the National Alert Service (NAS) in the postal and communication sectors. Since information security and CIIP is a horizontal issue that cuts across the responsibilities of individual government departments, Hungary has established a number of inter-ministerial bodies dealing with these tasks. In addition, the Theodore Puskas Foundation, a public-private partnership, plays an important role in CIIP, since it operates the national Computer Emergen*cy Response Team* (CERT-Hungary).

- In **India**, the National Information Board (NIB) consists of twenty-one members and is at the top of the national information security structure. Directly linked to the NIB is the National Technology Research Organization (Technical Cybersecurity) and the National Information Security Coordination Cell (NISCC), which is part of the National Security Council Secretariat (NSCS). The NISCC deals with CERT functions, R&D, encryption, laws, interception and early warning, cyber-crime, training and international cooperation. The NIB has instructed the NSCS to coordinate cyber-security activities across the country. It works through Sectoral Cyber Security Officers (SCOs). Directly below the NIB is the Information Infrastructure Protection Center (IIPC), followed by state cyber-police stations; the Computer Emergency Response Team India (CERT-In), and state and sectoral CERTs. Various ministerial coordinators of special functions are also situated at this level, as is the Development and Promotional Section of the Ministry of Communications and Information Technology (MOC). As a public-private partnership initiative, the Indo-US Cyber Security Forum strives to discuss and implement increasing cooperation in high-tech between the two countries.

- In **Italy**, the main Italian government bodies dealing with CIIP are the Ministry of the Interior (Postal and Communications Police) and the Ministry of Innovation and Technologies. The Postal Communication Police Service also hosts and manages emergency centres at both the national and regional levels, in order to deal more effectively with computer crime cases. The Ministry of Communication is also involved in various activities to improve the security of information and communication networks. In order to improve CIIP at all levels, public agencies also collaborate closely with the private sector. The most important public-private partnership in the field of CIP is the Association of Italian Experts for Critical Infrastructures (the Associazione Italiana Esperti in Infrastrutture Critiche [AIIC]), an expert group of practitioners from both the public and the private sectors.

- In **Japan**, the Cabinet Secretariat is the main actor in the field of CIIP and information security in general. It has an IT Strategy Council consisting of twenty opinion leaders.

In 2005, the Information Security Policy Council (ISPC) and the National Information Security Centre (NISC) were established within the Cabinet Secretariat, both now the focus of national CIIP policies. The ISPC, which plays a central role in developing and reviewing security strategies and policies, is chaired by the chief cabinet secretary and forms part of the IT Strategic Headquarters with members from various ministries and private-sector experts. The NISC is the central implementing body for IT security issues. The Cabinet Secretariat is assisted by the Ministry of Economy, Trade and Industry (METI), the National Police Agency (NPA), and the Ministry of Internal Affairs and Communications. METI is responsible for planning and implementing information policies under the guidance of the IT Strategic Headquarters, and deals with e-commerce, e-government, data protection, and R&D related to IT. The NPA maintains computer and network security and investigates cyber-crimes via its High-Tech Crime Technology Division (HTCTD), which is committed to preventing and minimising the spread of large-scale cyber-related incidents and to arresting cyber-criminals. One branch consists of mobile technical teams, stationed throughout Japan, led by a Cyber Force Centre. MIC is responsible for creating the national infrastructure and publishes an annual White Paper on Information and Communications in Japan. As a private-public partnership initiative, the CEPTOAR (Capabilities for Engineering of Protection, Technical Operation, Analysis, and Response) seeks to improve information-sharing between the government and the private sector.

- In the **Republic of Korea**, all governmental organisations and their subsidiaries are responsible for CIIP. The National Cyber Security Center (NCSC), which operates under the auspices of the National Intelligence Service (NIS), coordinates the efforts of these departments and agencies, serves as a platform that brings together the private, public, and military sectors to fight cyber-threats and is the central point of government for identifying, preventing, and responding to cyber-attacks and threats in Korea. For cyber-crime investigation and prevention, the Internet Crime Investigation Centre (ICIC), under the Supreme Public Prosecutors' Office plays a central role. The Electronics & Telecommunications Research Institute (ETRI) has leadership in developing technology and providing support to CIIP. The Ministry of Public Administration and Security (MOPAS), the Korea Communications Commission, the Ministry of Knowledge and Economy and the Korea Internet Security Center (KISC, KrCERT/CC) within the Korean Information Security Agency (KISA) foster a culture of safe Internet and telecommunication networks and share CIIP-related responsibilities. KISA includes an Information Infrastructure Protection Division with a CIIP Planning Team, a Critical Infrastructure Security Management Team, and the Korea Certification Authority Central Team. The National Information Security Alliance (NISA), consisting of twenty-two governmental organisations and information security officials from seventeen public enterprises, communication network providers, and experts from industry and academia, is a public-private partnership with the aim of improving information security by facilitating information exchange.

- In **Malaysia**, the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) administers security issues in the public sector, has an ICT Security Division, operates CERT for government, and is host of the Government ICT Security Command Centre, which monitors cyber-threats. The Ministry of

Science, Technology and Innovation (MOSTI) holds wide-ranging responsibilities concerning national ICT Policy, CIIP and cyber security. The Police Cyber Crime Unit is responsible for investigation and prevention of commercial cyber crime, while CIP is the responsibility of the Ministry of Energy, Water and Communications (MEWC). The Malaysian Communications and Multimedia Commission (MCMC) has a coordinating role and ensures information security, integrity and reliability of the network of Malaysia.

- In **The Netherlands**, responsibility for CII lies with a number of authorities, but the Ministry of the Interior and Kingdom Relations coordinates CIP/CIIP policy across all sectors, the work of the other responsible ministries, international policy, and national emergency management, which includes the National Crisis Centre. The General Intelligence and Security Service (AIVD) is also involved in protecting information security.

- In **New Zealand**, the Centre for Critical Infrastructure Protection (CCIP), located at the Government Communications Security Bureau, is the central institution dealing with cyber security and working with Critical National Infrastructure (CNI) organisations, industry and government to improve CIIP and computer security. CCIP aims to become a reliable and recognised source of information relevant to CNI protection, providing 24/7 watch and warning, and investigating and analysing cyber incidents. The main actor in charge of formulating New Zealand's security policy, including cyber security, is the Domestic and External Secretariat (DESS) – the support secretariat for the Officials Committee for Domestic and External Security Coordination (ODESC), which is chaired by the prime minister. The Government Communications Security Bureau (GCSB) gives advice and assistance to government departments and agencies concerning the security of information-processing systems and reports directly to the prime minister.

- In **Norway**, the national key player in civil emergency planning, the Directorate for Civil Protection and Emergency Planning (DSB), is also a key player for CIP/CIIP-related issues. It is subordinated to the Ministry of Justice and Police. The overall authority for ICT security is the Ministry of Government Administration and Reform. The Ministry of Defense is responsible for the military side. The Ministry of Transport and Communications has responsibility for the communication sector, including all security issues. The Norwegian National Security Authority (NSA) coordinates preventive IT security measures. The National Information Security Coordination Council (KIS) has no decision-making authority, but provides a platform for discussions and advises ministries and agencies in topics related to ICT security, CIP and CIIP. It consists of representatives from six ministries, the prime minister's office, and ten different directorates.

- In **Poland**, two ministries have responsibilities that relate to the country's information infrastructure and its protection – the Ministry of Science and Higher Education and the Ministry of the Interior and Administration. The main player and single coordinating body for science and technology policies is the Ministry of Science and Higher Education, which is involved in all policies relating to information infrastructures and their protection. It advises all ministries and institutions on ICT strategies and ensures compatibility of national public IT systems. The Ministry of the Interior and Administration is responsible for the national IT infrastructure, the national telecommunications system and the national information administrative systems.

- In **Russia**, the main organisations responsible for information security are the Security Council, the Federal Security Service (FSB), the Federal Guard Service, the Federal Technical and Export Control Service and the Ministry of Information Technologies and Communications. The Security Council defines Russia's national interests related to information, defines the resources that must be defended, and coordinates the elaboration of an information security strategy. The FSB safeguards the Russian Federation and CIIP. It has a Computer and Information Security Directorate in its Counterintelligence Service, plans and implements scientific-technical policy for information security, supports cryptographic and technical engineering security of ICT systems, protects state secrets and all types of communications. The Federal Guard Service has a Special Communications and Information Service which is now partly doing what FAPSI did until it was abolished in 2003, with its functions distributed between the FSB, the Guard Service and the General Staff. The Technical and Export Control Service, under the jurisdiction of the Ministry of Defence ensures information security in ICT systems, countering foreign technical espionage, and protects classified information. The Ministry of Information Technologies and Communications implements state policy in, and oversight over, the communications sector.

- In **Singapore**, the Singapore Infocomm Technology Security Authority (SITSA), a division within the Internal Security Department of the Ministry of Home Affairs (MHA), has the mission to secure Singapore's IT environment against threats to national security, such as cyber terrorism and cyber espionage and is responsible for operational IT security development and implementation at the national level. SITSA is hardening critical Infocomm infrastructure (CII) against cyber attacks and strives to achieve a higher level of national preparedness. Regulatory agencies continue to be responsible for IT security-related implementation for their sectors in coordination with SITSA. Responsibility for the government and infocomm sectors lies with the Infocomm Development Authority (IDA) in its capacity as the Government Chief Information Office (GCIO). The National Infocomm Security Committee (NISC) is the national platform to formulate IT security policies and set strategic directions at the national level with IDA serving as its secretariat.

- In **Spain**, the various aspects of CIP and CIIP policies mainly come under the auspices of the Ministry of Industry, Tourism, and Trade; the Ministry for Public Administration; and the Ministry of the Interior. There are two State Secretariats under the administration of the Ministry of Industry, Tourism, and Trade: the State Secretariat of Tourism and Trade and the State Secretariat of Telecommunications and for the Information Society. The latter is in charge of two General Directorates: the General Directorate of Telecommunications and Information Technologies (DGTTI) and the General Directorate for the Development of the Information Society (DGDSI). Three initiatives under the auspices of the Ministry for Public Administration are important with regards to Spain's information and communication infrastructure and its security: the e-Government Council, its Technical Committee, and the Technimap Project. The task of the e-Government Council is to prepare, elaborate, develop, and apply the government's IT policies and strategies and is elaborating a security policy in collaboration with the National Cryptology Centre of the National Intelligence Centre for the development of information and communication security measures and systems security. The Technical Committee for the Security of Information Systems and Personal Data Processing (SSITAD) is responsible for cyber-security and for supporting the e-Government Council. Technimap is a conference that brings together ICT experts from various areas of the public administration, the main companies in the field, and other experts. Under the auspices of the Ministry of the Interior, both the National Police and the Guardia Civil deal with cyber-crime. The National Police operates through the Information Technology Crime Unit and the Guardia Civil hosts a High Technology Crime Department. The National Police Department and the General Judicial Police Department have an emergency service for cyber-crime. The National Centre for the Protection of the Critical Infrastructures (CNPIC) is responsible for leading, coordinating, and supervising the national CIP. Moreover, there are two public-private partnerships in the field: the Information Society and Telecommunications Analysis Center/ENTER, and AETIC, the Spanish Electronics, Information Technology and Telecommunications Industries Association.

- In **Sweden**, a number of organisations are involved in CIP/CIIP. In 2009, the Swedish Civil Contingencies Agency (MSB) in the Ministry of Defence was tasked to submit proposals for the prevention and handling of IT incidents in Sweden by January 2010. It intends to set up a National Operational Coordination Centre for cyber security at the agency. The fundamental purpose of the Centre will be cooperation between government agencies with operational assignments in information security and to be a central part of the crisis management system. The Emergency Management Agency (SEMA) at the Ministry of Defence also has an important role. In addition, there is a Joint Action Group for Information Security (SAMFI) directed by the MSB, comprising representatives from the Armed Swedish Forces, the Swedish National Defence Radio Establishment (FRA), the Swedish Post and Telecom Agency (PTS), and the Swedish National Police Board. Within the Cabinet Office, cross-departmental work is being performed on ways to implement the findings of SEMA and to reform CIIP in Sweden. The public-private partnership initiatives in Sweden currently include SEMA's efforts to promote interaction between the public and the private sector, the Industry Security Delegation (NSD) and the Swedish Information Processing Society (DFS)

- In **Switzerland**, there are a number of different organisational units dealing with CIP/CIIP. One of the main bodies on CIIP is the Federal Strategy Unit for Information Technology (FSUIT). Part of the Federal Department of Finance, it produces instructions, methods, and procedures for information security, is responsible for the Special Task Force on Information Assurance (SONIA), and for the Reporting and Analysis Centre for Information Assurance (the Melde- und Analysestelle Informations-sicherung [MELANI]) that has a key role with the Cybercrime Coordination Unit (the Koordinations-stelle zur Bekämpfung der Internetkriminalität [KOBIK]) both within the Federal Office of Police (FEDPOL). The Federal Office of Information Technology, Systems, and Telecommunications (FOITT) is also part of the Federal Department of Finance and is responsible for security and emergency preparedness for the federal administration's IT systems at the operational level. There is also an ICT Infrastructure Unit of the Federal Office for National Economic Supply, the Federal Office for Civil Protection (FOCP) responsible for CIP, and the GovCERT. On the military defence side is the Führungsunterstützungsbasis (FUB). Public-private partnerships are among the central pillars of Switzerland's CIIP policy.

- In the **United Kingdom**, the Cyber Security Strategy 2009 stresses the need for a coherent approach to cyber security in which the government, organisations across all sectors, the public and international partners have a part to play. It called for two new organisations (both operational by March 2010). The first of these is the Office of Cyber Security (OCS) under the Cabinet Office to provide strategic leadership for and coherence across government. It will also have a role in coordinating cyber-offence capabilities that build on resources existing in MoD, the intelligence services and the police (Metropolitan Police e-Crime unit, the Child exploitation and Online Protection Centre, and the Serious and Organized Crime Agency, Soca). The second new body is the Cyber Security Operations Centre (CSOC) based at GCHQ in Cheltenham that brings together existing functions to monitor the health of cyber space, coordinate incident response, enable better understanding of attacks against UK networks and users, and provide advice and information about risks to business and the public. The Centre for the Protection of National Infrastructure (CPNI) also runs a CERT-service which responds to reported attacks.

Annex 2.

International and Regional Responses[45]

The Council of Europe

The Convention on Cybercrime (CETS 185), elaborated by the Council of Europe with the participation of Canada, Japan, South Africa, and the US, opened for signature in Budapest in November 2001 and has been in force since July 2004. It is open for accession by any country and is the only binding international treaty on the subject to have been adopted to date. The Protocol on Xenophobia and Racism Committed through Computer Systems (CETS 189) opened for signature in January 2003 and has been in force since March 2006.

The Convention requires signatory nations to create the basic legal infrastructure required to address cyber crime effectively and to commit to assisting other signatory nations in investigating and prosecuting cyber criminals. Scope of the Convention includes: criminalising conduct; illegal access to a computer system; illegal interception; data interference; system interference; misuse of devices; computer-related forgery and fraud; child pornography; infringement of copyright and related rights; and tools for efficient investigations and safeguards. It applies to any offence committed by means of a computer system and to any evidence in electronic form.

The Convention has twenty-eight ratifications (EU countries plus the US); forty-six signatories (EU countries, Canada, Japan, and South Africa, all NATO member countries); five states invited to accede (Chile, Costa Rica, Dominican Republic, Mexico, Philippines); and several notable non-signatories (China and Russia). It is used as a guideline, reference standard or model law in more than 100 countries. In addition, the Convention is supported and referred to by other organisations, including: the European Union; Organisation of American States; OECD; Asia-Pacific Economic Cooperation; Interpol; and members of the private sector.

Although there has been broad international acceptance of the Convention, some have criticised it as insufficient to properly handle acts with national security implications. First, the Convention treats attacks on IT systems as criminal offences against private and public property, thereby disregarding the national security dimension of such attacks. Second, it does not differentiate between attacks on ordinary computer systems and those on critical infrastructure information systems, or between small and large-scale attacks.

Nonetheless, the Convention represents a basic but essential piece of international legislation. It provides a sound set of legal and technical definitions upon which additional agreements for enhanced cooperation may be developed. Since there is a significant overlap between cyber crime, cyber terrorism, and cyber warfare, the Convention's criminalisation of all acts of cyber attack, regardless of motivation, means that it requires signatories, when requested, to apprehend and hand over for prosecution all international cyber attackers, regardless of their definition by host nations as criminals, terrorists, or even praiseworthy patriots.

[45] The information in this annex was kindly contributed by Mr. Fred Schreier

The European Union

The EU is a key player at the international level concerning information assurance. CIIP, the Information Society, and information security are considered key issues. The EU has launched initiatives and research programmes to study various aspects of the information revolution and its impact on education, business, health, and communications.

The Communication of the Commission of the European Communities (EU Commission) on *Critical Infrastructure Protection in the Fight against Terrorism,* adopted on 20 October 2004, provides a definition of CI, enumerates the critical sectors identified, and discusses the criteria for determining potential CI. In the follow-up publication of the EU Commission, the *Green Paper on a European Program for CIP* of 17 November 2005, CIIP is defined. In 2008, the European Commission launched a policy initiative on CIIP.

Among other initiatives and policies are:

- Study for the Commission on the Availability and Robustness of Electronic Communication Infra-structures (ARECI)
- Critical Infrastructure Warning Information Network (CIWIN)
- European Network and Information Security Agency (ENISA) created in March 2004, started operations in September 2005 in Crete. The challenge for ENISA is to help achieve a high EU-wide level of security in electronic communications.
- TESTA: Trans-European Service for Telemetrics between Administrations. Constitutes the EU's own private network, isolated from the Internet and allows officials from different ministries to communicate at a trans-European level in a safe way.

EU Initiatives in the R&D domain include:

- Information Society Technologies (IS) FP6 and FP7
- European Security Research Program (ESRP)
- Critical Information Infrastructure Research Coordination (CI2RCO)
- Service and Software Architectures, Infrastructures, and Engineering

Relevant EU Laws and Legislation include:

- Data Protection Directive 1995
- Directive on Electronic Signature 1999
- Directive on Privacy Protection in the Electronic Communications Sector 2002
- Framework Directive 2002
- Council Framework Decision on Attacks Against Information Systems 2005
- Directive on Data Retention 2006

The Forum of Incident Response and Security Teams (FIRST)

FIRST, formed in 1990, is the only worldwide global Forum for Incident Response and Security Teams. The organisation is widely recognised as a global leader in incident response and brings together a variety of Computer Security Incident Response Teams (CSIRTs) from government, commercial, and education organisations. It aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information-sharing among members and the community at large.

Group of Eight (G8)

Since 1995, the Group of Eight (G8) has become increasingly involved in issues relating to cyber-crime, the Information Society, CIP and CIIP. At the Halifax summit in 1995, a group of senior experts was given the task of reviewing and assessing existing international agreements and mechanisms to fight organised crime. This G8 Senior Experts Group took stock before drawing up a list of forty operative recommendations, which were approved at the G8 summit in Lyon in 1996. This Lyon Group has since developed into a permanent multidisciplinary body with numerous specialized sub-working groups. Since October 2001, the Lyon Group meetings have been held together with the Roma Group on combating terrorism.

A further important stage for the G8 and CIP/CIIP came in spring 2000, when government officials and industry participants from G8 countries attended the G8 Paris Conference on Dialogue Between Public Authorities and Private Sector on Security and Trust in Cyberspace. The aim was to discuss common problems and to find solutions associated with high-tech crime and the exploitation of the Internet for criminal purposes. The G8 member states agreed on defining a clear and transparent framework for addressing caber-crime. They adopted principles that aim to foster the emergence of a new "security culture", strengthen international cooperation, and encourage implementation of the best professional practices in the field of computerized surveillance and alert. They proposed the conducting of common exercises to test the reaction capabilities in case of incidents, to make other countries aware of the problems, and to invite them to adopt the same main courses of action. The eleven principles are intended to guide national responses to CIIP.

The essential elements of the principles of protecting CII were adopted by the 78th UN General Assembly in Resolution 58/199 of January 2004, entitled "Creation of a global culture of cyber security and the protection of critical information infrastructures."

North Atlantic Treaty Organization (NATO)

NATO started its cyber defence programme in 2002 after incidents in the late 1990s related to operations in the Balkans. As a result of this experience, NATO leaders at the 2002 Prague Summit directed that the technical NATO Cyber Defence Program be implemented, establishing the NATO Computer Incident Response Capability (NCIRC). With a NCIRC Coordination Centre at NATO Headquarters in Brussels and a NCIRC Technical Centre in Mons, NATO has equipped itself with the means to delivering several critical tasks, from the detection and prevention of computer viruses and unauthorized intrusion into NATO networks, to the management of cryptographic devices for the Internet.

In addition, NATO experts provide technical support for computer security incidents as well as policy and forensic devices. Apart from the establishment of the CCD Center of Excellence in Estonia, NATO has also created a Cyber Defence Management Authority (CDMA), operational since April 2008 and charged with initiating and coordinating "immediate and effective cyber defence action where appropriate." At the NATO Summit in Strasbourg/Kehl in April 2009, member states pledged to accelerate the acquisition of new cyber defence assets, make cyber defence an integral part of NATO exercises and strengthen the linkage between NATO and partner countries on protection against cyber attacks. Most recently, NATO officials have confirmed the development of Rapid-Reaction Teams to be made available to member states to counter cyber attacks.

CIP remains one of the key areas of work related to Civil Emergency Planning in NATO. The Ministerial Guidance for NATO Civil Emergency Planning includes several references to CIP, while the updated Civil Emergency Planning Action Plan for the improvement of civil preparedness against possible chemical, biological, radiological, and nuclear attacks includes several action items related to the CIP field of work. The Senior Civil Emergency Planning Committee and its eight planning boards and committees continue to examine CIP from a functional perspective, and to provide integrated contributions from the areas of expertise of all Planning Boards and Committees.

A *Special Report to the NATO Parliamentary Assembly 2007* and subsequent reports on NATO and cyber defense (173 DSCFC 09 E bis) outlined the critical infrastructure policies of NATO and individual member countries. It contains the various definitions, highlights their commonalities and differences, and attributes responsibilities by identifying the CIP stakeholders and the sectoral policies including CIIP, energy security, civil aviation security, and port security.

Organisation for Economic Co-operation and Development (OECD)

The OECD has a long history of expertise in developing policy guidance for the security of IT systems and networks, including CIIP. It is also committed to the fight against cyber crime and, in particular, the use of malicious software. The OECD produces analytical reports, statistics, policy declarations and recommendations to help governments and businesses develop consistent policies to strengthen information security, to raise public awareness about the importance of information security and, more broadly, to develop a culture of security across society. There is consensus among the member countries that secure and reliable information infrastructures and services are a necessary requirement for trustworthy e-Commerce, secure transactions, and personal data protection. This is the main reason why the OECD Working Party on Information Security and Privacy (WPISP) promotes a global approach to policymaking in these areas, with the aim of building trust online. In addition, the Committee for Information, Computer and Communications Policy (ICCP) analyses the broad policy framework underlying the e-Economy, information infrastructures, and the Information Society.

United Nations (UN)

Issues related to CIIP have been discussed by the UN since the end of the 1980s. However, formal CIIP efforts are a more recent phenomenon. Several initiatives have since been undertaken towards better work coordination. Among these are initiatives taken by the UN institutions, several UN resolutions, and the results of the World Summits on the Information Society (WSIS).

The UN Institute for Disarmament Research (UNIDIR) conducted workshops on how to better achieve worldwide information security and assurance in a global digital environment. And the UN Office on Drugs and Crime has been advocating a broad, inclusive focus to address problems of cyber crime through joint training events.

In December 2000 and 2001, the 55th and 56th General Assemblies issued Resolutions 55/63 and 56/121 on "Combating the criminal misuse of IT." In December 2002, the 57th UN General Assembly issued Resolution 57/239 on the "Creation of a global culture of cyber-security." In December 2003, the 58th UN General Assembly issued Resolution 58/199 on the "Creation of a global culture of cyber-security and the protection of critical information infrastructure." The resolution's annex outlines eleven principles for CIIP. In subsequent years, the UN General Assembly regularly adopted a resolution on "Development in the field of information and telecommunications in the context of international security." In 2005 and 2006, two subsequent resolutions on WSIS were adopted.

The establishment of the UN ICT Task Force in November 2001, in response to a request by the UN ECOSOC, was a further important step. The task force was mandated to mobilise worldwide support for attaining the Millennium Development Goals with the use of ICT. In April 2004, a seminar on "Policy and security issues in information technology" was held at the UN Headquarters. In 2005, the taskforce published a guide called "Information Insecurity – A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security," which attempted to create greater awareness about the growing dangers of cyber hooliganism, cyber crime, cyber terrorism, and cyber war.

At the WSIS, world leaders entrusted the International Telecommunication Union (ITU) with a leading role in coordinating international efforts on cyber security. As the sole facilitator for the action line related to Building Confidence and Security in the Use of ICT, the ITU launched the Global Cyber-security Agenda (GCA) in May 2007 to provide a framework within which the international response to the growing challenges to cyber-security can be coordinated and addressed. The GCA benefits from the advice of a High-Level Expert Group comprising more than 100 world-renowned specialists in cyber-security from governments, industry, international organisations, research organisations and academia. In 2007 and 2008, the ITU carried out significant standardisation work in security architecture, encryption and authentication, and information security management systems. In addition, it has launched the ICT Security Standards Roadmap, an online database that provides information about existing ICT security standards and works in progress in key standard development organisations.

The World Bank Group

The growing incidence of computer and cyber-crime has particularly strong bearings on the financial sector. In view of the growing amount of financial data stored and transmitted online, the ease of computer intrusions has added to the severity of the problem. Therefore, the World Bank Group has taken several steps over the last few years to face the challenges of information security, especially in developing countries.

The Global Information and Communication Technologies Department (GICT) promotes access to ICT in developing countries and serves the World Bank Group's core departments for research, policy, investment and programmes related to ICT.

The *Information Technology Security Handbook*, published in 2003, provides technology-independent best practices and recommendations in the field of IT security. As the technology evolves, the accompanying website provides updates as appropriate.

The World Bank published a report on *Electronic Security: Risk Mitigation in the Financial Transactions* in June 2002, building on previous papers that identified e-security as a key component to the delivery of e-finance benefits. In January and May 2004, a follow-up publication was published, entitled Technology Risk Checklist, which describes thirteen layers of e-security, covering both hardware and software pertaining to network infrastructures. These layers cover risk management, policy management, cyber-intelligence, access controls and authentication, firewalls, active content filtering, intrusion detection systems, virus scanners, encryption, vulnerability testing, systems administration, incident response plans, and wireless security. In 2005, two further documents were published by the e-security/e-finance section on the larger dangers emanating from BOTs, cyber parasites, and on the issue of money laundering in cyberspace.

The EastWest Institute Worldwide Cybersecurity Initiative

In 2007, the EastWest Institute's Strategic Dialogue team from the US led by General (ret.) James Jones, former SACEUR and now US National Security Advisor, challenged senior Chinese and Russian leaders in discreet talks to break the deadlock in international cooperation in meeting cyber security challenges. Intense Track 2 discussions followed at high levels. All three governments confirmed the concerns each holds for the intentions and actions of the others. It also showed a deep-seated common concern over the growing capacity of non-state actors to wreak havoc upon global economic stability, as well as begin to pose serious security challenges. Each of the big three had already changed their estimates regarding cyber security, with the US raising it to the same level as nuclear security.

Today, these three countries are working together in a Worldwide Cybersecurity Initiative (WCI) managed by the EastWest Institute. They have been joined by leading figures from the EU and other G20 nations, the private sector, professional associations and international organisations.

The Advisory Group of WCI is led by General Harry Raduege, Chairman of the Deloitte Centre for Cyber Innovation. The vision is two-fold: (1) build trust by tackling specific cyber security problems together in discreet bilateral or multilateral teams; and (2) begin a public process that will enable the first steps to be taken in international cyberspace policy much as they have been undertaken relative to the sea, air, and outer space. This EWI initiative begins its public phase in May 2010 when 200 leaders from the "Cyber 40" nations (the G20 and the other twenty most important cyber nations) will come together in Dallas for the first Worldwide Cybersecurity Summit sponsored by EWI. This first effort to create a movement of the public and private sector will focus on protecting critical cyber security infrastructure (finance, energy, telecoms and essential government services).

About the series

A great deal of material has been produced on the rise of private military and security companies (PMSCs). Recent work has also sought to integrate these actors into a wider SSR and SSG agenda. However, there is, as yet, very little that takes the logical next step and explores the role of a wider range of private and other non-state actors in responding to a broad range of security governance challenges. We will be obliged in the years to come to broaden our analytical horizons way beyond current SSR and SSG approaches. There is a growing urgency to move beyond the first revolution in this area that led to the "whole of government" approach towards a second revolution, one that leads to a fully integrated security sector approach that reaches beyond established state structures to include select private companies – and thus permit, what we might call, a "whole of issues" approach.

This project brings together relevant state and non-state actors for a series of thematic roundtables throughout 2010. Each roundtable is designed to inform a subsequent working paper. These working papers provide a short introduction to the issue, before going on to examine theoretical and practical questions related to transparency oversight, accountability and democratic governance more generally. The papers, of course, do not seek to solve the issues they address but rather to provide a platform for further work and enquiry. As such, they ask many more questions than they answer. In addition to these working papers, the project has published an occasional paper – *Trends and Challenges in International Security: An Inventory* – that seeks to describe the current security landscape and provide a background to the project's work as a whole.

The Geneva Centre for the Democratic Control of Armed Forces (DCAF) is one of the world's leading institutions in the areas of security sector reform and security sector governance. DCAF provides in-country advisory support and practical assistance programmes, develops and promotes appropriate democratic norms at the international and national levels, advocates good practices and conducts policy-related research to ensure effective democratic governance of the security sector.

Visit us at: www.dcaf.ch

DCAF Geneva
P.O. Box 1360
1211 Geneva 1
Switzerland

Tel: +41 (22) 741 77 00
Fax: +41 (22) 741 77 05

DCAF Brussels
Place du Congrès 1
1000 Brussels
Belgium

Tel: +32 (2) 229 39 66
Fax: +32 (2) 229 00 35

DCAF Ljubljana
Dunajska cesta 104
1000 Ljubljana
Slovenia

Tel: +386 (1) 5609 300
Fax: +386 (1) 5609 303

DCAF Ramallah
Al-Maaref Street 34
Ramallah / Al-Bireh
West Bank, Palestine

Tel: +972 (2) 295 6297
Fax: +972 (2) 295 6295

DCAF Beirut
P.O. Box 113 - 6041
Beirut
Lebanon

Tel: +961 (1) 738 401
Fax: +961 (1) 738 402