sandfire

Analysis Consulting Technology Training

Analysis

Securing Cyberspace

Building Blocks for a Public-Private Cooperation Agenda

Heiko Borchert and Felix Juhl

About the Authors

Heiko Borchert is Managing Partner of Sandfire, a Swiss expert consultancy for public-private security advice, advisory board member of IPA Network in Berlin, and a subject matter expert at the Hague Centre for Strategic Studies. He is co-editor of a series of books on networked security and member of the editorial board of the Zeitschrift für Aussen- und Sicherheitspolitik. He has studies international relations, business administration, law, and economics at the University of St Gallen, Switzerland, where he also received his Ph.D. His main areas of work include critical infrastructure protection, public-private security cooperation, energy security, and security sector transformation.

Felix Juhl is Senior Partner of Sandfire and expert on open source intelligence, lawful communication interception, cyber security, counter-espionage, and fighting organized crime. After serving in the German Bundeswehr he held several top management positions in the consulting and IT industry. From 2006-2009 he ran his own company that provided technology solutions for governments and law enforcement agencies in many different countries. Prior to joining Sandfire's management team in 2011, he worked at the Center for Security Studies at the Swiss Federal Institute of Technology (ETH) in Zurich.

Paper to be published in Josef Schröfl, Bahram Rajaeed, and Dieter Muhr (eds.), Hybrid and Cyber War as Consequences of the Asymmetry (Vienna: Peter Lang International, forthcoming).

Sandfire AG Bruchmattstrasse 12 CH-6003 Lucerne
Phone +41 41 312 07 40 Fax +41 41 312 07 44 www.sandfire.ch info@sandfire.ch

Overview

Securing Cyberspace
Building Blocks for a Public-Private Cooperation Agenda

Heiko Borchert and Felix Juhl

Abstract
In the 21st century, access to the global commons – sea, air, space, and cyberspace – will be contested. The growing interrelationship between operations in each of the global commons puts a premium on cyber security as the key link. Therefore, cyber insecurity is not only a technical problem. Rather, it is a strategic concern as cyber insecurity threatens to rip modern societies off the benefits of accessing the global commons. This paper looks at ways to improve the trustworthiness of cyber infrastructures and cyber-related services. It starts with a discussion of key cyber-related concepts and finds that the lack of agreed definitions is a stumbling block for international collaborative efforts to provide cyber security. Then the paper puts forward a generic framework to analyze cyber vulnerabilities. Against this background the paper concludes by advocating a comprehensive approach to deal with cyber security. To this purpose the paper presents six areas for public-private security cooperation in cyberspace.

The prosperity of modern societies depends on the free flow of people, goods, resources, and information. To assure these free flows, global movement management is key.[1] Global movement management essentially depends on the openness of the global commons, i.e., sea, air, space, and cyberspace.[2] Historically, openness entails unrestricted access to, maneuverability within, and use of the global commons. Today, the rise of non-state actors and the proliferation of technology, growing demand for mineral and energy resources, international power shifts from the hitherto dominant transatlantic region to the Asian theater, and long-term trends such as demographic developments and climate change encroach upon the openness of the global commons. As a consequence, the 21st century will see a growing contest between different actors to access the global commons and shape them according to their specific interests.

In the global commons, cyberspace plays a special role. Unlike the other elements of the global commons, cyberspace is the product of deliberate action by men. It consists of various hardware and software components that have been woven together in a global network. Thus, cyberspace can change rather rapidly, whereas conditions in the maritime environment, air space, and space are relatively constant.[3] Nowadays, the seamless functioning of cyberspace has become the single most important prerequisite for operations in all glob-al commons. Cyberspace is a key enabler for actions in other domains of operations and has become an operational domain of its own.[4]

Cyberspace is hybrid in nature. It is neither owned nor operated exclusively by public or private actors. Because cyberspace is the glue that binds together single actions by individuals, states, and companies, everyone has a stake in securing it. Therefore, advancing cyber security requires close public-private interaction. This, however, is easier said than done. Today's cyber security governance – the rules, norms, principles, structures, and processes that guide interaction between different actors – is hardly adequate to deal with known and foreseeable cyber security risks. For too long, the existing division of responsibility between ministries, public agencies, cyber-infrastructure owners and operators, and users of cyber-dependent services has remained unchanged. This is not a minor problem, as inadequate cyber security governance risks eroding the benefits modern societies receive from access to the global commons.

This article analyzes current and future cyber risks and puts forward concrete suggestions to make cyberspace more secure. First, we will look at different definitions and concepts such as cyber security, cyber crime and cyber terrorism, and cyber war and cyber deterrence that serve as the most important paradigms today. The problem with all of these definitions is

1 For more on this, see: W. Scott Gould, Daniel B. Prieto, and Jonah J. Czerwinski, *Global Movement Management: Commerce, Security, and Resilience in Today's Networked World* (New York: IBM, 2007).

2 For an introduction to the literature on global commons, see: Barry R. Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security,* 28:1 (Summer 2003), pp. 5-46; Michèle A. Flourney and Shawn Brimley, "The Contested Commons," *Proceedings,* 135:7 (July 2009), <http://www.usni.org/magazines/proceedings/2009-07/contested-commons> (access 2 November 2010); Abraham M. Denmark and James Mulvenon (eds.), *Contested Commons: The Future of American Power in a Multipolar World* (Washington, DC: Center for a New American Security, 2010); Scott Jasper (ed.), *Securing Freedom in the Global Commons* (Stanford: Stanford Security Studies, 2010).

3 Greg Rattrey, Chris Evans, and Jason Healey, "American Security in the Cyber Commons," in Denmark/Mulvenon (eds.), *Contested Commons,* p. 143.

4 Mark E. Redden and Michael P. Hughes, "Global Commons and Domain Interrelationships: Time for a New Conceptual Framework?," *Strategic Forum* No 259 (Washington, DC: National Defense University, 2010).

the basic assumption of attribution, i.e. establishing a clear cause-effect chain between individual actions and observed effects. This is hardly the case in cyberspace, which provides an area of almost complete anonymity. Thus restricting anonymity in cyberspace becomes important, but also raises thorny political, legal, and conceptual issues. Second, we provide an overview of the most important cyber vulnerabilities. This overview will underline the need for comprehensive cyber security approaches. We will conclude with a six-point working agenda to advance public-private cyber security cooperation.

Cyber Confusion: Making Sense of Different Concepts

Defining cyber-related issues and distinguishing between various cyber phenomena is crucial to our task. Definitions provide a common language necessary for sound collaboration and meaningful discussion. Furthermore, definitions help determine the scope of the problem to be addressed and are necessary for clear communication about a subject. Today, however, cyber-related definitions are vague at best, which causes confusion. We start by looking at some of the key terms currently in use.

Cyber security

The most well known term is cyber security. Traditionally, cyber security is discussed in terms of vulnerabilities, threats, and countermeasures. Computers and networks are critical for key functions such as managing and operating nuclear power plants, dams, electric power grids, air traffic control systems, almost any distribution of supplies and energy, as well as the financial infrastructure. Companies, organizations, governments, and individuals rely on computers as they do on electronic communications, which are evidently enabled by computers. The majority of computer systems are networked via globally connected computer networks known collectively as the Internet. More recent trends point towards embedding computing capability in all kinds of devices and environments as well as integrating network
embedded systems into larger systems.[5] As a consequence, computer and communication systems are critical components of modern infrastructures and have become critical infrastructures of their own.

In terms of information security and trust in information systems, users of cyber infrastructure components and services have three distinct needs:

- Confidentiality: the right to control and authorize who can read what kind of information.
- Integrity: the capability to assure that information and software programs are modified only in specified and authorized ways.
- Availability: continued access to information and cyber services by authorized users.

As we will outline in the next section, these needs are threatened by different cyber vulnerabilities stemming from technical, organizational, regulatory, economic, human, and even natural origins. This broad understanding leads to a basic definition of cyber security, which is understood as all necessary ends, ways, and means to protect computer systems and data against unauthorized accidental or intentional intrusion, disclosure, transfer, modification, or destruction.

[5] *Making the Nation Safer. The Role of Science and Technology in Countering Terrorism* (Washington, DC: National Academy Press, 2002), pp. 135-176.

Against this background it makes sense to separate three different forms of cyber insecurity:

- Vulnerability, which is an error or weakness in the design, implementation or operation of a system.
- Threats that stem from activities by perpetrators who want to exploit vulnerabilities of electronic systems and are capable to do so.
- Risks that entail the likelihood that vulnerabilities will be exploited or threats may cause harm.

In addressing these issues it is very important to keep in mind the complex interplay between the origins of cyber insecurity and related countermeasures. Vulnerabilities, threats, or risks prompt specific countermeasures, but these very countermeasures may themselves spawn new cyber insecurities. Therefore a holistic approach to designing cyber security solutions is needed.

Cyber crime and cyber terrorism

Crimes committed in or via cyberspace are commonly referred to as cyber crime. The growing number of publications dealing with cyber crime illustrates that the notion has become popular. But despite the broad use of the term, [6] it is very difficult to define the concept properly.

First of all, current definitions of cyber crime are not based on the deduction of generic categories, but tend to focus on single use cases or observed effects (e.g., phishing). In addition,
there is no catch-all expression to describe all the tools and software applications that are used to commit online crimes. Different sorts of Trojans, Viruses, Bots, Spyware, and Worms are instrumental in facilitating various forms of cyber crime. This, in turn, affects every aspect of prevention, remediation, and law enforcement. Keeping these aspects in mind, cyber crime can be understood as any kind of crime facilitated or committed by using software applications, computers, networks, or hardware devices. Thus the notion of cyber crime encompasses a very broad and diversified continuum of offenses.

This understanding leads to a clear differentiation between cyber crime and cyber terrorism. Cyber terrorism is the combination of terrorism and cyberspace. It is generally understood to describe unlawful attacks and threats of attack against computers, networks, and the information stored therein. The purpose is to intimidate or coerce a government or its people to give in to particular political or social objectives. Moreover, to qualify as cyber terrorism acts should either cause harm to generate fear or result in violence against people or property (e.g., severe economic loss, contamination of water and food supply systems, explosions, plane crashes, bodily injury, or deaths). Depending on their impact, serious attacks against critical infrastructures could qualify as acts of cyber terrorism as well. By contrast, attacks that disrupt non-essential services or are a costly nuisance would most likely not qualify as cyber terrorism.

[6] Combating the criminal misuse of information technologies, United Nations, General Assembly Resolution 56/121, A/RES/56/121, 23 January 2002, <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf>; Combating the criminal misuse of information technologies, United Nations, General Assembly Resolution 55/63, A/RES/53/63, 22 January 2001, <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf> (access 5 November 2010).

Cyber war and cyber deterrence

The revolution of information technology has prompted new approaches to modern warfare. The modern battlefield has become wired with computers connecting individual soldiers to the overall command and control systems, controlling targeting systems, relaying critical intelligence information to users in distributed networks, and managing logistics to name but a few examples. While this trend creates obvious advantages such as improving joint situational awareness and joint situational understanding or shortening the Observe-Orient-Decide-Attack loop, it also creates new vulnerabilities. Reliance on commercial computer and information technology makes armed forces vulnerable to the same kind of cyber risks that also hamper civilian users.

Given the armed forces' reliance on information and communication technology, cyber war is about to become standard practice. However, predicting the effects of cyber war attacks is undermined by the same complexity that makes these kinds of attacks possible in the first place. Investigations in the run up to a cyber war attack may reveal that a particular system has specific vulnerabilities. But exploiting these vulnerabilities requires in-depth knowledge about the behavior of the system and its processes under attack and the response of the system and its operators if signs of dysfunction are detected. Collecting these insights in advance or parallel to conducting cyber war attacks is demanding. This makes it difficult to assess the real potential and limits of military cyber attacks. Therefore it is worth taking a look at different intentions:

- **Strategic intention**
  In this case the prime motive is to seriously affect an opponent's will and capabilities. Think for example of a cyber strike against an opponent's critical infrastructures meant as a clear sign that the cost of intervention abroad would be felt sharply at home. A strategic cyber attack might be carried out against the main military forces of an opponent (e.g., state) to cripple its capabilities temporarily and buy time for other actors to organize their forces in other global commons.

- **Operational intention**
  In this case cyber attacks could be used to affect the capabilities of an opponent engaged in ongoing hostilities. The main purpose is to delay or stop the opponent's battle rhythm.

- **Special intention**
  Cyber attacks conducted with a special intention in mind are designed to achieve particular effects that are limited in time, scope, and impact. A special cyber attack would most likely occur outside the context of physical combat and in covertness. Examples could include attempts to hobble a state's nuclear weapons production, address a high-value target such as an individual leader, and taking down or affecting hostile websites. The purpose of special cyber attacks is analogous to special operations conducted in other domains.

- **Psychological intention**
  Causing deliberate confusion could be another intention to launch cyber attacks. The main rationale would be to limit the ability of others to carry out cyber attacks on their own. But given the mixed signals sent by the original cyber attack, the opponent would have a hard time figuring out the real motives behind being attacked. Techniques used

to conduct cyber attacks to cause confusion may scratch the fringe line between defense, offense, and espionage.

Most cyber war attacks that have been observed so far only lasted a few seconds.[7] The effects caused by these attacks may last much longer, but in most cases it took only a few seconds to inject malware, for example. Therefore cyber war experts believe that cyber warfare is only a supporting element in military operations. But there is more to the use of cyber war attacks. Not only military powers are maintaining efforts in cyber attacks and cyber capabilities, organized crime organizations and terror groups operate their own cyber commands and cells around the world. This prompts a new need to collect information about cyber warfare capabilities of non-state actors.

In parallel to the evolution of the theory and practice of cyber war, a growing body of literature deals with cyber deterrence.[8] In essence, deterrence is about psychology. Deterrence takes place in the mind of an opponent. He or she will determine whether actions by someone else have a deterring effect. This requires the necessary capabilities in order to credibly impose a danger to the other. In addition, someone who wants to deter an opponent must effectively convey his message to the other. As a consequence, deterrence will most likely not work if the wrong "language" is used, the wrong party is addressed, or if ambiguous, misleading, insincere, or indeterminate messages are conveyed.

And this is where cyber deterrence starts to get difficult. The inherent anonymity of cyberspace greatly complicates attribution of responsibility for an attack or the threat of an attack. Therefore it is difficult to hold perpetrators accountable for specific action. Any alleged violation could simply be met with a strongly worded denial, and unambiguous evidence supporting the allegation would be hard to provide. Moreover, behavioral norms are generally much harder to instill and enforce in an environment in which actors can act anonymously. The problem occurs in the target's mind. Given the anonymity of cyberspace, it is hard if not impossible to recognize if a cyber operation should be interpreted as an effective attack or as a "simple" message demonstrating the opponent's capability to launch the respective attack. Moreover, in cyberspace deterrence is no longer the prerogative of nation states. At least in theory, individuals have the potential power at their fingertip to cause serious harm. This, however, makes it even more difficult to design and launch legitimate, proportionate, and appropriate responses.

Cyber Vulnerabilities and Challenges

So far, security research has been focusing on formal policy models that protect information against unauthorized access by specifying which users should have access to data or objects. Today's multilayered and asymmetrical cyber risks challenge the paradigm of "absolute security" and gives rise to a model built on axioms of insecurity: insecurity exists; insecurity cannot be overcome; and security can be circumvented. As a consequence, there is a need for a generic approach towards the different dimensions of cyber vulnerability.

[7] For an excellent discussion of cyber war attacks, see Eneken Tikk, Kadri Kaska, and Lils Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn: Cooperative Cyber Defence Centre of Excellence 2010), pp. 14-33.

[8] See for example: Martin Libicki, *Cyberdeterrence and Cyberwarfare* (Santa Monica: RAND, 2009), Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice?," *Strategic Studies Quarterly,* 4:3 (Fall 2010), pp. 102-135.

Figure 1 illustrates four different environmental spheres.

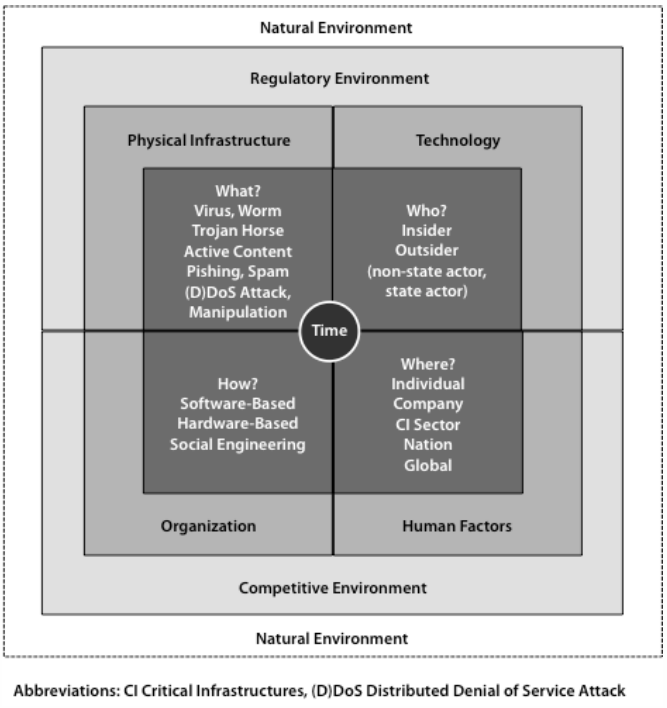

Figure 1: Generic Cyber Vulnerability Dimensions

At the center, the dark shaded core illustrates the four core cyber vulnerabilities segments: What are the tools and methods of attack or manipulation? Who is the mischief? Where is the impact about to be felt? How is the operation about to be conduct? Temporal dynamics, which may spread from milliseconds to weeks, are part of all four segments. Not every Virus or Worm will become active or infect hosts instantly. New breeds of Malware can wait for external orders or can download further code prior to becoming a threat to the environment. This makes it difficult to establish cause-effect chains to prepare appropriate responses.

Potential threats are well documented through research and court cases because of fraud, sabotage, negligence, human error, and exploitation caused by different perpetrators. When addressing the role of perpetrators the focus tends to be on outsiders. This, however, is problematic, as many cases of cyber operations conducted by insiders demonstrate. Different actors ranging from individuals to groups of people or nation states can commit illicit cyber acts. As we will argue in the final section, anonymity in cyberspace makes it difficult to identify if only one actor is launching an activity or if a group of people is engaged. As far as threat vectors are concerned, the risk of social engineering (i.e., establishing or exploiting interpersonal relations to receive information not readily available) should receive more attention. In this regard, observance of online social communities will gain in importance.[9] Finally, the geographic range of deliberate cyber activities can vary extensively from private Local Area Networks to networks of companies, critical infrastructure sectors, and governments. All four segments depend on each other, as a successful attack or intrusion requires at least one or more of these elements.

9 *Social Networking. The security shakedown of shared information* (The Hague: The Hague Centre for Strategic Studies, 2010).

The second sphere takes into account the immediate environment in which cyber infrastructure components are used. References to technology make clear that cyber dangers evolve dynamically in tandem with cyber-relevant technology progress (e.g., could computing). Innovations in other science and technology fields (e.g., quantum science and technology, power and energy techniques, or materials technology) should also be kept in mind because the combination of innovation in various fields could provide new risks and opportunities for cyber applications. Human factors also highlight the key role of human beings in a techno-centric world; despite the focus on technical solutions to keep pace with cyber risks, human factors should not be disregarded. Ignorance, negligence, or bad faith remains key sources of cyber vulnerabilities. This makes it clear that education, awareness building, and personnel background checks continue to play an important role as basic security measures.[10] In addition, today's organizational environment poses significant cyber-relevant vulnerabilities of its own. Among others, these results from the advancement of distributed networks that allow for flexible project structures across continents and highly fragmented global supply chains. As a consequence, the use of cyber applications must be tightly coordinated with organizational development. Finally, there is the physical infrastructure that can be affected by cyber incidents. But the physical infrastructure itself also has an impact on cyberspace. Think, for example, of the growing technical shortage of bandwidth capacity essential to communications.

The remaining two spheres describe the broader operating environment in which cyber applications are embedded. The regulatory and legal environment is key. Cyberspace presents itself as a unified domain, but the regulatory environment is in fact highly fragmented in terms of the norms, rules, and principles that should be followed. This is probably one of the most important stumbling blocks for the effective abatement of cyber-related vulnerabilities. Regulatory variations create cyber vulnerabilities because they create regulatory loopholes that can be exploited by perpetrators. And regulatory differences can provide disincentives for companies to invest in cyber security. Regulatory problems are reinforced by today's competitive environment. Cost consciousness, for example, is one of the reasons for the increased use of commercial off-the-shelf (COTS) components in public and private sectors.[11] COTS comes with the advantage of proven usability, but in most cases IT and security staffers do not know what kind of COTS components have been used, where they are coming from, and if these components are reliable. There is a growing number of system components whose functionality can be changed remotely and unnoticed while the system is operating. Administrators cannot know with certainty what software was used to build the components and what commands these components might execute. Taken together, the pressure on costs and concerns about the intensions of certain technology owners creates a new set of security questions that will be addressed in the final section of this paper.

Last but not least, there is the natural environment. Because physical cyber infrastructure components are located in the natural environment, there is a direct link between natural phenomena such as underwater earthquakes or storms in space and the functioning of the cyberspace. Problems resulting from the impact of climate changes on physical cyber infra

[10] See also: *Emerging Cyber Threats Report 2011* (Atlanta. Georgia Tech Information Security Center, 2010), pp. 6-7.

[11] In 2007, the US Defense Science Board rang the alarm bell when a study revealed the extensive proportion of open source or COTS code lines in defense-critical software. See: *Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2007).

structure are likely to get worse if current projections about global climate change turn out to be correct.

A Public-Private Working Agenda to Advance Cyber Security

Nowadays, politicians and practitioners agree that cyber security requires close public-private interaction. However, the need for public-private security cooperation[12] is not only limited to cyber security. Given economic globalization and the growing dependence of the state on private contractors and private infrastructure operators, national security and corporate security are becoming ever more intertwined. In reality, however, public-private security cooperation is hard to achieve because existing institutional boundaries, organizational cultures, and legal regulations most often work to the detriment of close relationships between ministries, agencies, and the corporate sector. This is a serious challenge, because failure to fill the rhetoric of public-private partnerships with life will serve as a further disincentive to cooperate. Against the background of our analysis the remainder of this paper is devoted to six issues that could constitute a public-private working agenda to advance cyber security.[13]

Reviewing Cyber Security Governance

Cyberspace was built to withstand all sorts of interruptions. Thus it is anarchic by nature. This creates unique governance problems. From a national security perspective, the most important problem stems from the fact that cyber-related issues run counter to existing national security bureaucracies. In most countries, the Ministries of the Interior and Justice play a key role. These institutions are experts at setting norms and legal frameworks, but they hardly have the technical capabilities to deal with cyber risks. This is where the national defense and intelligence establishment comes in. But the specter of interfering with individual privacy makes it difficult to fully exploit cyber-related defense capabilities.

Given the public sector's difficulties in organizing itself, it is hardly surprising that it is difficult for the private sector to find adequate inroads into the public community in order to address cyber issues. For example, many countries have organized dialogues with the private sector along the thematic responsibilities of various ministries. Owners and operators of critical infrastructures maintain established lines of communication with the respective supervisory authorities in their respective field of action. Cyber security, by contrast, requires a horizontal approach that cuts across existing stovepipes.

In reorganizing national security structures to deal with cyber-related issues, there is no "one size fits all" approach. Some countries refer to "cyber czars" whereas others appoint lead Ministries to provide for the necessary coordination. Whatever approach is chosen, it will be important to follow a comprehensive approach. Comprehensiveness starts by recognizing that many other actors must be brought on board in addition to the traditional defense and security establishment. Infrastructure Ministries play a key role, because they provide the basis for national infrastructure plans. Ministries of Economics are indispensible in advancing trust in electronic commerce. Energy Ministries and energy market supervisory authorities

[12] Our understanding of public-private security cooperation is not restricted to the outsourcing of state functions to private contractors. Rather we look at the whole "life cycle" of activities encompassing joint analysis, strategy development and implementation, conduct of operations, financing, education and training, research and development, and procurement and maintenance.

[13] For additional suggestions, see also the papers by Walter Unger, Kurt Einzinger, and Nemanja Malisevic in this volume.

are important to address the cyber dimension of smart grids and smart electricity meters. Ministries for Research and Education should join as well in order to provide for holistic cyber research activities, raise awareness for cyber issues in education programs, and help develop tomorrow's cadre of cyber experts.

In addition, it is important to reorganize key processes such as strategic foresight, strategy development, controlling, finance, and human resources across organizational boundaries in the public and private sectors. Strategic foresight provides the necessary information for the early detection of new threats pertaining, for example, to technology developments or changes in social behavior that could lead to new forms of using cyber applications. The other four processes are key to cyber-related management, and here things start to get turf-bound. In the end, finance and human resources are the high grounds of any organization. If, however, there is no consensus on a joint provision of funds and experts commensurate with overall strategic guidelines, the successful implementation of cyber security strategies will be seriously hampered.

The whole-of-government approach to deal with cyber issues needs to be complemented by "bringing the private sector in." Many countries have established information exchanges to share intelligence information about threats and disseminate best practice. Public-private cyber security exercises to test and evaluate existing plans, concepts, and capabilities to deal with cyber risks create added value as well.[14] In addition, the private sector should step up joint efforts to analyze and address cyber vulnerabilities within and beyond industry sectors and along global supply chains. Although Business Continuity Management is becoming standard practice in the private sector, studies show that there is room for improvement in looking at cyber-related supply chain disruptions, analyzing the preparedness of upstream and downstream supply partners, and evaluating the readiness of business-critical suppliers to withstand cyber incidents.[15]

Bringing together all relevant stakeholders to advance cyber security is one aspect of cyber security governance. In addition, it is also necessary to clarify individual and collective responsibilities. To this purpose, a public-private working group should

- Map out and analyze who is affected by cyber incidents and what are the consequences of these incidents;
- Assess the impact of cyber incidents on public-private and civil-military relations in order to identify the level of defensive and offensive capabilities needed to react adequately;
- Draft a primer on legal aspects for public-private interaction between armed forces, law enforcement, intelligence services, and the private sector to respond to cyber incidents and conduct investigations (e.g., address issues of hot pursuit; set priorities in terms of mitigation versus investigation);
- Establish a joint understanding on thresholds for government action (e.g., identify when cyber incidents constitute an armed attack; discuss the legitimacy, appropriateness, and proportionality of different actions commensurate with the nature of the original cyber

[14] In November 2010, the European Network and Information Security Agency conducted the first pan-European cyber security exercise "Cyber Europe 2010," <http://www.enisa.europa.eu/media/press-releases/cyber-europe-20102019-cyber-security-exercise-with-320-2018incidents2019-successfully-concluded> (access 5 November 2010).

[15] *A Decade of Living Dangerously. The Business Continuity Management Report 2009* (London: Chartered Management Institut, 2009).

incident; elaborate on the use of sanctions and applying other forms of coercive non-military power).

Strengthening Collaborative Efforts to Create Cyber Domain Awareness (CDA)

Successful operations require joint situational awareness and joint situational understanding. This holds true for operations in all domains, and thus also in the cyberspace. As we have argued, CDA is difficult to achieve because of the technical characteristics of cyberspace. Therefore it should receive more attention by public and private actors.

CDA is important to accomplish many different tasks. First, it helps detect network intrusion and suspicious behavior in cyberspace. Among other things, this refers to the coverage of authorized and unauthorized devices that are connected to cyber networks or the monitoring of data flows between network components and users. Second, CDA is indispensible in coordinating the activities of different actors as outlined above. Without a clear understanding of who is doing what in case of a cyber incident, it will be difficult to organize adequate response. This is particularly true for the often-neglected issue of unintended side effects. Imagine a scenario where one actor acts on early warning information and bolsters its defensive posture. How can we make sure that all actors operating in cyberspace perceive these measures as defensive? Let's assume further that this actor's defense also includes taking offline and restricting access to specific cyber services. Do we know in advance what the cascading effects of these actions will look like? Third, we believe that CDA will become paramount to monitor the spillover of cyber risks from the electromagnetic domain to the physical domain. This is a lesson to be learned from the most recent Stuxnet incident.

One approach to advance CDA is to build on the idea of operational pictures that have been set up in maritime, space, and air domains. The basic purpose of any operational picture is to provide an overview of all relevant actors in the respective theater of operations and beyond. In doing so, it is key to distinguish between friendly and adversarial forces and identify likely intensions and available capabilities. The same logic also informs CDA-related technology developments. These include projects to find and identify devices in open or restricted networks according to IP addresses, recognize Malware by their behavior, provide databases of computers that are infected by viruses, which would help provide early warning on infected computers before they become active.[16]

Addressing the Challenge of Attribution and Identity Management in Cyberspace

Authentication in cyberspace is difficult, because it is relatively easy to operate anonymously in the cyber domain. An attacker wanting to cause damage will compromise intermediary targets whose vulnerabilities are easy to detect and exploit. These targets will be used to launch more serious attacks against the ultimate target. In order to tackle authentication challenges, much emphasis is placed on identity management.

Identity management can be understood as "the combination of technical systems, rules, and procedures that define the ownership, utilization, and safeguarding of personal identity information. The primary goal of the identity management process is to assign attributes to

[16] "Spotting malware by its signature. Digital DNA compares RAM, stored data to find viruses," *Defense News,* 17 May 2010, p. 24; "Endgame, virus-buster," *Intelligence Online,* 11 March 2010, p. 8; "Mapping the Pentagon's networks. DoD uses IPSonar to improve defenses," *Defense News,* 18 January 2010, p. 16.

a digital identity and to connect that identity to an individual."[17] The basic idea is that each user could use a single and secure identity to benefit from different cyber-related services rather than taking recourse to many different security measures to authenticate his or her identity.[18] In doing so, biometric identification based for example on facial recognition or iris scans can help establish a clear link between an individual and his or her (electronic) identity. This information can then be used to verify a user's authority to access an electronic system or retrieve information from databases. The same information can also be used to monitor exchanges in online communities or intercept telecommunication in order to identify potential perpetrators.

Identity management is important, but not enough. Figure 1 has made it clear that user-related as well as hard- and software-related aspects must go hand in hand in order to make cyberspace more secure. Identity management helps improve user authentication. But the ultimate challenge is to ensure that the underlying information technology is effectively secured and resistant to malicious software of various types. Strong identification will not compensate for information technology that is poorly designed, configured, and/or operated. Indeed, vulnerabilities in the underlying technology will threaten the integrity of an identity management scheme. Therefore more joint efforts are needed to build security into overall cyber architectures and into the underlying components needed for the cyber domain.

Advancing the Use of Predictive Analytics

Predictive analytics and sequence prediction are the Holy Grail of preventive security policy. But is it possible to predict cyber threats or attacks against secure information, infrastructures, and systems? Many security sensors and systems can be deployed to provide defense-in-depth for systems and networks. However, the sheer volume of security alerts poses challenges for security operators in analyzing an attack and launching appropriate responses. Alert correlation and analysis is a critical task in security management. Therefore, a standard low-level correlation should be complemented with new algorithms, techniques, and tools for security analysts to further analyze and correlate attack scenarios in order to properly assess situations and missions and take appropriate counter-measures that minimize damages. In addition, threat analysis and attack prediction are also helpful and important for security operators to take preventive action.

Recognizing attack plans is a premier goal of security analysts, and "plan recognition" has long been a research area in artificial intelligence. Plan recognition describes a process of inferring the goals of an intruder or attacker by observing his or her activities. In advancing our capabilities to recognize plans, in cyber war we must first acknowledge that observed attacker activities most often do not match existing pre-defined attack plans. Second, plan recognition assumes a complete, ordered set of tasks for a plan. However, given the difficulties of attribution, one cannot always observe all of the attacker's activities. Too often, detection of attack activities is incomplete due to limits in the performance and distribution of sensors. Therefore, an attack plan recognition system should have the capability to deal with known attack vectors, standard routines, algorithms and code lines, tools and mechanisms, and unobserved but monitored or intercepted activities. Even Malware and Viruses have

[17] *Identity Management Task Force Report 2008* (Washington, DC: National Science and Technology Committee, 2008), p. ES-1.

[18] For more on this, see also: *National Strategy for Trusted Identities in Cyberspace. Creating Options for Enhanced Online Security and Privacy* (Washington, DC: The White House, 2010).

their own signature. Experts can compare this information with existing knowledge bases to track intruders or at least the close-by region of origin.

Different approaches have been suggested to security alert correlation and attack scenario analysis. For example, Xinzou Qin has proposed a "probabilistic-based correlation engine that incorporates domain knowledge to correlate alerts with direct causal relationships" in order to "filter out unrelated attacks, correlate security alerts, analyze attack scenarios and take appropriate actions against forthcoming attacks."[19] Many different technologies and concepts are emerging like deep packet inspection, threat intelligence and real-time network forensic systems, meta data, visualization or direct analysis as well as pattern and sequence prediction. The ITU Toolkit for Cybercrime Legislation addresses these issues. Since threats can originate anywhere around the globe, challenges are inherently international in scope and require international cooperation, investigative assistance, and common substantive and procedural provisions. Thus, it is important that countries harmonize their legal frameworks to combat cyber crime and facilitate international cooperation.[20]

These challenges related to attack plan recognition open the door for fruitful public-private research and technology cooperation. To start with, current approaches are based on predefined attack plans built on security experts' knowledge and understanding of networks and systems under protection. If attackers' activities are beyond the predefined scope of attack plans, we must act quickly to identify new attack vectors and come up with counter-measures that are commensurate with the new situation. Another challenge addressed above is how to distinguish deceptive plans from real goals and intensions of attackers. This highlights the need to develop mechanisms that help identify real intentions and unveil deceptive operations by attackers. Finally, we also need to consider how to effectively distinguish between attacks conducted by single attackers and groups of attackers working together. All of these activities might require the establishment of a trusted test environment in which different approaches can be validated under real conditions.[21]

Bolstering Trust in Cyber Hardware Components

We tend to equate cyber insecurity with software problems. This is hardly surprising because each of us has most likely encountered problems with Viruses, Worms, and other software-related problems. Most recently, however, the number of reports dealing with untrustworthy cyber hardware is growing. While software can be patched, this is hardly the case for hardware.[22] The vulnerabilities of the hardware that underpins the global cyberspace are thus a fundamental security challenge.

Cyber hardware insecurity, among other things, can result from counterfeit products such as network components. If counterfeit network components are part of a nation's critical cyber

19 Xinzhou Qin, *A Probabilistic-Based Framework for INFOSEC Alert Correlation* (Atlanta: Georgia Institute of Technology/College of Computing, 2005).

20 <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf> (access 5 November 2010).

21 This is the key idea behind the National Cyber Range program developed by the Defense Advanced Research Projects Agency (DARPA) in the US. See: William J. Lynn, "Defending a New Domain," *Foreign Affairs,* 89:5 (September/October 2010), pp. 97-108, here pp. 105-106.

22 Wesley K. Clark and Peter L. Levin, "Securing the Information Highway. How to Enhance the United States' Electronic Defenses," *Foreign Affairs,* 88:6 (November/December 2009), pp. 2-10.

infrastructure or its security and defense systems, this becomes a crucial problem.[23] In addition, hardware insecurity can be the result of strategic calculations by peer competitors. The most prominent example is the growing suspicion about Chinese telecommunication operator Huawei that is said to maintain strong bonds with electronic warfare experts of the People's Liberation Army. Countries such as the United States, the United Kingdom, France, and India have voiced concern about attempts of Huawei to enter their respective telecommunication markets, as its products are believed to have secret back doors that allow for the unwanted siphoning off of sensitive data.[24]

Bolstering and reestablishing trust in cyber hardware will require public-private cooperation along three different avenues. First, there is a need to follow cyber hardware components through the global supply chain, a challenge that is itself multidimensional. Global competition based on exploiting cost advantages prompts manufacturers to outsourcing thus making oversight of an already fragmented global supply chain for cyber hardware even more difficult. In addition, the degree of oversight that would be required is neither contractually nor culturally the job of component manufacturers.[25] State security agencies, industrial users, and manufacturers thus need to work together more closely to secure the supply chain of cyber hardware components. This will require the seamless exchange of information for early detection of counterfeit components and best practice to counter economic espionage.

Second, securing the cyber hardware supply chain also requires vendor and manufacturer screening in order to certify the authentication and reliability of their products. This could, for example, also include new provisions on hardware-related risk management as part of public and private procurement regulation.[26] In addition, industry and governments should consider establishing a joint knowledge base to identify "who owns whom" in order to avoid the purchase of hardware components from manufacturers that maintain relations with dubious state and non-state partners.

Third, manufacturing capacity should be addressed as well. Observers raise concerns about the fact that the vast majority of key components such as integrated circuits are provided by Chinese suppliers.[27] This could give rise to the idea of re-establishing national manufacturing capacities for certain key components in order to reduce dependence on dubious foreign suppliers. Public and private sector experts should consider the feasibility of this idea in particular for components used in key national and international critical infrastructure components and national security and defense systems.

Identifying Critical Cyber Infrastructure Components

The final issue that should be addressed jointly is the role of critical cyber infrastructures. Critical infrastructure is a concept that addresses the vulnerability of modern societies

23 Clark/Levin, op. cit., p. 8; "Counterfeit chips may hobble advanced weapons," *Homeland Security News,* 30 October 2009; "Fake chips from China threaten U.S. military systems," *Homeland Security News,* 9 September 2010;

24 "Unease grows as Chinese telecom behemoth gains foothold in U.S.," *Homeland Security News,* 27 October 2010; "Pentagon seeks tight ties with cyber contractors," *Reuters,* 21 October 2010; "China has the keys," *Intelligence Online,* 25 February 2010; "Warning Over Chinese Eavesdropping on Border," *Intelligence Online,* 4 June 2009, p. 4; "Spy chiefs fear Chinese cyber attack," *Sunday Times Online,* 29 March 2009.

25 *Cyber Threats to National Security. Countering Challenges to the Global Supply Chain* (Arlington: CACI, 2010), p. 12.

26 Op. cit., p. 17.

27 Op. cit., p. 16.

resulting from infrastructure failure or disruption. So far, the European Program on Critical Infrastructure Protection is focused on the energy and transport sectors and looks at infrastructures in EU member states only. But there are strong indications that information and communication technology could be addressed as an additional sector in the future.[28]

Considering the role of international critical cyber infrastructures in this overall equation raises the obvious question of how these infrastructure components will be identified. As we have argued above, there are many different elements that constitute cyberspace. One could look at Internet exchanges as one example of international critical cyber infrastructures. Internet exchanges are relevant for the exchange of Internet traffic by Internet service providers. Open source information reveals that some of the world's busiest Internet exchange points are operated in Europe.[29] If one or more of these exchange points fail to operate properly at the same time, digital data transfer within and beyond Europe could be affected. [30] The question, however, is if and to what extent the capacities of these Internet exchanges could be substituted.

Substitution is also a case in point for other key parts of the global cyber infrastructure: undersea cables and satellites. Both are important to handle global data traffic, but they are also prone to specific risks. These include natural hazards, ignorance or malfunction, and deliberate action to interrupt data transfer. Like many other cyber infrastructure components private actors operate undersea cables and satellites. This leads to the next question: What should be done in case one of these cyber infrastructure components is identified as internationally critical? Who is in charge of the safety and security, and who pays for it? Answers to these questions are beyond the scope of this paper, but it is obvious that the right incentives must be in place for private actors to invest in adequate safety and security measures.

In addition to the physical and electromagnetic vulnerability of cyber infrastructure components, ownership and operation of these elements should also be addressed. Raising this issue is tricky, because it could be seen as an attempt to turn back market liberalization and restrict competition on the ground of national security concerns. But in the case of cyber infrastructures we should keep in mind that cyber infrastructure providers can directly access data transported along these infrastructures. As information is key in today's globalized world, concerns about information breaches enabled by the ownership and operation of key cyber infrastructure components should be taken seriously. Therefore we see a need for public-private information exchange in terms of the multi-faceted corporate and non-corporate networks behind alliances and joint ventures that have been established to provide the relevant cyber infrastructure components. We also recommend reviewing existing and (if needed) adopting new procedures to screen investments in national and international critical cyber infrastructures in order to avoid corporate takeovers that unintentionally affect national security.

Finally, we should also keep in mind the mutual dependence of different sectors. Cyber security is relevant for other sectors, but actions in other sectors also influence cyber security. The advancement of smart grids as part of a larger transformation of today's energy

[28] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection, Official Journal of the European Union, L345, 23 December 2008, pp. 75-82; Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, COM(2009)149 final, Brussels, 30 March 2009. For more on the European program, see also the paper by Walter Unger in this volume.

[29] <http://en.wikipedia.org/wiki/List_of_Internet_exchange_points_by_size> (access 3 November 2010).

[30] Rattray/Evans/Healy, "American Security in the Cyber Commons," p. 168.

sectors toward the use of more eco-friendly energy resources is one example. Smart grids build on the idea of connecting different devices to a common energy network in order to produce, transfer, and store energy. This could open doors to new cyber risks as smart meters can be hacked or infected with Viruses.[31] Smart grids would also allow electric cars to go online to reload and provide additional storage capacities. However, electronic control units of today's cars are not yet fit enough to deal with deliberate attacks and could thus be used as new inroads to destabilize cyberspace.[32] Another interesting example is high frequency stock or bond trading. This practice depends on high-performance infrastructures to execute a large amount of trades in microseconds. Whereas high frequency trading may offer attractive economic incentives, computer security practice is said to be lax. This could facilitate interception to manipulate trades and cause damage beyond the stock markets.[33]

31 "Experts say smart meters are vulnerable to hacking," *Homeland Security Newswire,* 30 March 2010; "Smart Grids still not immune to cyber attacks," *Homeland Security Newswire,* 29 October 2009.

32 "Ausser Kontrolle. Hacker-Angriffe aufs Auto," (Out of Control. Hacker Attacks against Cars) *Neue Zürcher Zeitung,* 27 May 2010, p. 59.

33 "High-frequency traders: Spread betting," *The Economist,* 14 August 2010, p. 56-57; "High-frequency traders get into piracy," *Intelligence Online,* 22 July 2010, p. 8.