DCAF HORIZON 2015 WORKING PAPER NO. 4

CYBER SECURITY: THE ROAD AHEAD

FRED SCHREIER, BARBARA WEEKES, THEODOR H. WINKLER

GENEVA SECURITY FORUM

10 DCAF

DCAF HORIZON 2015 WORKING PAPER NO. 4

CYBER SECURITY: THE ROAD AHEAD

FRED SCHREIER, BARBARA WEEKES, THEODOR H. WINKLER

GENEVA
SECURITY FORUM

10
DCAF

Table of Contents

Abstract

The open Internet has been a boon for humanity. It has not only allowed scientists, companies and entities of all sorts to become more effective and efficient. It has also enabled an unprecedented exchange of ideas, information, and culture amongst previously unconnected individuals and groups. It has completely revolutionized on a global scale how we do business, interact and communicate.

Cyberspace is defined by its ubiquitous connectivity. However, that same connectivity opens cyberspace to the greatest risks. As networks increase in size, reach, and function, their growth equally empowers law-abiding citizens and hostile actors. An adversary need only attack the weakest link in a network to gain a foothold and an advantage against the whole. Seemingly localized disruptions can cascade and magnify rapidly, threaten other entities and create systemic risk.

However, vulnerabilities in cyberspace are real, significant and growing rapidly. Critical national infrastructure; intelligence; communications, command and control; commerce and financial transactions; logistics; consequence management; and emergency preparedness are wholly dependent on networked IT systems. Cyber security breaches, data and intellectual property theft know no limits. They affect everything from personal information to national secrets.

This paper looks at the way these problems are likely to develop, as well as at some of the ways they may best be tackled at the national and international level.

1. The Issues

1.1 Cyberspace

Cyberspace, the 5th space of warfare (after land, sea, air, and space) consists of all of the computer networks in the world and everything they connect and control via cable, fibre-optics or wireless.[1] It is not just the Internet—the open network of networks. Cyberspace includes the Internet plus many other networks of computers, including those that are not supposed to be accessible from the Internet. Some of those private networks look just like the Internet but they are, theoretically at least, separate. Other parts of cyberspace are transactional networks that do things like sending data about money flows, stock market trades, and credit card transactions. In addition, there exist supervisory control and data acquisition systems that allow machines to speak to other machines, like control panels talking to pumps, elevators and generators. This is also known as the "Internet of things", within which inanimate objects can communicate with each other, often with the help of RFID technology (radio frequency identification).

Cyber criminals can hack into these networks and control or crash them. If they take over a network, they could steal all of its information or send out instructions that move money, spill oil, vent gas, blow up refineries, pipelines and generators, derail freight and metro trains, crash air-traffic control systems, send troops into an ambush, or cause a missile to detonate prematurely or in the wrong place. If they crash networks, wipe out data, and turn computers into passive warriors (botnets), then financial systems could collapse, supply chains could be interrupted, the electric power grid could blackout, satellites could spin out of orbit into space, and airlines could be grounded. A loss of confidence in financial data and electronic transfers could cause economic upheaval. A loss of power lasting just a few days could produce a cascade of economic damage as money runs out and food becomes scarce.

Things like this have happened, some experimentally, sometimes by mistake, and others as a result of cyberwar or cybercrime. Information managed by computer networks, which run energy utilities, transportation, banking and finances, communications, healthcare, private and corporate data, and state secrets can be exploited or attacked from remote locations. Many things in cyberspace make this possible, including flaws in the design of the Internet; flaws in hardware and software; the move to put ever more critical systems online; the lack of effective deterrents; and the absence of appropriate defence mechanisms. Threats in cyberspace are as broad and diverse as cyberspace itself. They derive from the nature of networks—their interconnectedness, scale, speed, and the challenge of comprehending precisely what is happening in any particular instance. Nothing can defend against cyber attacks with convincing certainty, located not only beyond borders but beyond physical space, in

[1] All images used in this publication are freely available on a creative-commons licence from Paul Garland, Dea Peajay, Miskan, Nico Kaiser and Anaxila.

the digital ether of cyberspace. Expanding bandwidths make it possible to propagate attacks at a much faster pace, even before organisations start patching their systems to protect themselves. As a result, it is increasingly cheap to launch destructive cyber attacks anonymously, but ever more expensive to defend against such attacks. This growing asymmetry is the real game changer. The modern thief can steal more money with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb. And these problems are persistent and unlikely to change soon.

1.2 Cyber crime

Cyber crime is a clear and present danger that has turned into a silent global digital epidemic. Cyber crime encompasses a wide range of offences, including hacking of computers, data and systems, computer-related forgery and fraud such as phishing and pharming,[2] content offences such as child pornography, and copyright offences via dissemination of pirated content. It has evolved from the mischievous one-upmanship of cyber vandals to a range of profit-making professional criminal enterprises in a remarkably short time. And there is a rapidly growing nexus between cyber crime and a variety of other threats, including industrial espionage, foreign intelligence services and terrorism.

As with other aspects of globalisation, the rapid expansion of the Internet has far exceeded regulatory capacity. And this absence of authority has opened space for more abuses. Cyber crime attacks are increasing in frequency, complexity and sophistication, with discovery ever more often occurring only after the fact, if at all. Cyber criminals are targeting organisations and individuals with malware and anonymization techniques that can evade current security controls. Current perimeter-intrusion detection, signature-based malware, and anti-virus solutions are providing little defence and are ever more rapidly becoming obsolete. Thus, cyber criminals are leveraging innovation at a pace which many targeted governments, organisations and security vendors can no longer match.

Moreover, cyber criminals can now target the weakest link in most security models (the end user) through the Internet by means of social engineering techniques. They use scams and ruses to make an end user believe they are co-workers, customers, or other legitimate parties. Steadily evolving stealth techniques enable them to act without fear of timely detection, let alone capture and successful prosecution.

Cyber attacks using malicious software have increased at an alarming rate in the last three years. Most of those attacks are aimed at the financial sector, and are hosted on financial sector computers.[3] Other forms of cyber crime, particularly intellectual property violations, may be more attractive to other criminal groups.

[2] Phishing and pharming are two popular forms of fraud that aim to dupe victims into believing they are at a trusted website such as their bank, when in fact they have been enticed to a bogus website that intends to steal their identity and drain their financial resources.

[3] Economic and Social Council, ECOSOC/6444, 37th & 38th Meetings, Council briefed on Cybersecurity, 16 July 2010, p. 1.

There are organised cyber crime groups of some longevity that prefer operating in areas like software piracy and other forms of copyright infringement.

An increasing number of malware authors and cyber criminals for hire now provide skills, capabilities, products and outsourced services to other cyber criminals. These include data acquisition and storage, stealthy access to systems, identity collection and theft, misdirection of communications, keystroke identification, identity authentication, and botnets. Among the great advantages cyberspace offers to criminals are anonymity, and the ability to allow otherwise unassociated individuals in different parts of the world to network on a transactional basis. In this way, an underground economy has evolved around stealing, packaging, and reselling information.

There are at least three reasons why cyber crime in general and organised cyber crime in particular will further increase in the near future. First, the technology of cyber crime has become more accessible. Software tools can be procured or purchased online that allow the user to locate open ports or overcome password and other protections. Such tools allow a much wider range of people to become offenders, not just those with a special gift for computing. For example, the proprietors of the recently discovered "Mariposa" botnet, perhaps the largest in history so far, had no advanced hacking skills.[4] Second, the profile of Internet users is changing. In 2005, the number of Internet users in developing countries surpassed the number in industrialised countries. Even if these new users may not be more likely predators than those in developed countries, the number of predators should continue to expand, while the number of high-value victims located in richer areas will remain more or less the same. As a result, the intensity of attacks on this victim pool will likely grow, since the Internet and broadband communication have made high-value victims as accessible as local ones for predators in the developing world.

Third, offenders can now increase the number of attacks exponentially through use of automation and growing bandwidth. Many millions of unsolicited bulk spam messages can be sent out by automation within a short time frame. Hacking attacks are now also automated with as many as 80 million incidents every day due to the use of software tools that can attack thousands of computer systems in hours. A recently detected botnet of 12.7 million infected computers, among them many in the world's biggest corporations, launched millions of automated attacks.[5] Among other things, schemes like this allow cyber-thieves to fly under the radar by taking only a small amount of money from a large number of victims, decreasing the chances of detection.

The losses posited to cyber crime vastly exceed the cost of other crimes, including drug trafficking. According to some estimates, the losses to society are between €750 billion[6] and 1 trillion US $ annually[7]—costs that may be understated because of a

[4] Charles Arthur, "Alleged controllers of 'Mariposa' botnet arrested in Spain," Guardian, 3 March 2010.

[5] UNODC, The Globalisation of Crime. A Transnational Organised Crime Threat Assessment, Vienna, 2010, p. 204.

[6] The European Commission says governments and society lose some €750 billion a year, and rising. Officials at Europol and at the European Network and Information Security Agency, Enisa, hesitate to put a figure on the cost, because of a lack of a single Europe-wide definition of cyber crime and its constant growth.

[7] UNODC, op. cit., p. 204. This includes losses due to intellectual property theft, and involves losses to companies, rather than

relative lack of accurate information about actual intrusions and associated financial losses.[8] However, there are concerns as to how representative these estimates are.

A growing threat:

Despite constant warnings about the vulnerabilities of IT equipment and the Internet, and many billions of dollars spent on defending electronic networks, the risk of cyber crime attacks continues to grow unabated. The growing threats and increasing number of reported intrusions on computer systems of government agencies and commercial companies highlight the vulnerabilities of the interconnected networks as well as the need to adequately address the global security and governance of cyberspace. The global aspects of cyberspace present key challenges to the security of all states. Until these challenges are comprehensively addressed, states will continue to be at a disadvantage in promoting their national and economic security, and the safety and security of their population in the realm of cyberspace. Trends in cyber crime demand a much more serious response:

- Cyber crime attacks and security breaches will increase in frequency, complexity and sophistication, with discovery increasingly occurring only after the fact, if at all.
- Most indicators point to future cyber crime attacks becoming more severe, more complex, and more difficult to prevent, detect, and address.
- Effective deterrents to cyber crime are not known, not available or not accessible to a majority of practitioners, many of whom still underestimate the scope and severity of the problem.
- Lack of accurate intrusion reporting to regulators and law enforcement is the core reason that issues related to cyber security and cyber crime are not being recognized as the most immediate priority.

1.3 National Cyber Security: core issues and strategic challenges

The open Internet has been a boon for humanity. It has not only allowed scientists, companies and entities of all sorts to become more effective and efficient. It has also enabled an unprecedented exchange of ideas, information, and culture amongst previously unconnected individuals and groups. It has encouraged new forms of production, notably "open source" methods, in which groups of people from all over the world develop and create new services and products collectively. It has completely revolutionized on a global scale how we do business, interact and communicate.

Cyberspace is defined by its ubiquitous connectivity. However, that same connectivity opens cyberspace to the greatest risks. As networks increase in size, reach, and function, their growth equally empowers law-abiding citizens and hostile actors. An adversary need only attack the weakest link in a network to gain a foothold and an advantage against the whole. Seemingly localized disruptions can cascade and magnify rapidly, threaten other entities and create systemic risk.

gains to cyber criminals.

[8] When cyber crime strikes, less than half of all victims call their financial institution or the police and just over a third contact the website owner or e-mail provider. Norton Cyber crime Report: The Human Impact, Symantec Corporation, Mountain View, 2010.

Vulnerabilities in cyberspace are real, significant and growing rapidly. Critical national infrastructure; intelligence; communications, command and control; commerce and financial transactions; logistics; consequence management; and emergency preparedness are wholly dependent on networked IT systems. Cyber security breaches, data and intellectual property theft know no limits. They affect everything from personal information to national secrets.

Hostile actors vary in scope, scale, intent, source, and resources. They can include foreign governments, intelligence services, and militaries; well-organised and funded non-state actors such as organised crime and terrorist groups; individual hackers and criminals; as well as disgruntled employees or other insiders. All of them can leverage cyberspace to inflict physical damage and disable critical portions of the digital infrastructure.

The strategic challenges:

- The threats to cyber security are the greatest national and economic security threats states face. Cyber security will evolve into a key challenge, economically, politically, socially, and militarily. Yet it remains the least understood and most underestimated threat.
- The very complexity of the threat deters a full understanding of its implications and hinders a comprehensive debate on the strategic responses needed.
- Cybersecurity is a cross-cutting issue that permeates all aspects of the life of a modern society and economy. This renders the identification of the specific problems posed and measures required more difficult.
- The ability to misuse, manipulate, or even dominate cyberspace will increasingly attract organised crime
- Cyber space needs to be understood increasingly as the most important theatre of military operations. The quest for cyber dominance—and the corresponding ability to protect against cyber attack—heralds a new era in military affairs, which will profoundly alter the nature and structure of military forces. Cyber will, in the foreseeable future, replace kinetic energy as the key component of military power.
- The omnipresence of cyber issues in modern life will require not only military answers to the threat, but a fully integrated strategy by the entire security sector. The growing importance of cyber will thus be among the major driving forces for security sector reform—and among the most complex challenges for security sector governance.
- Cyber security cannot be achieved at the level of the nation state alone. It requires fully integrated responses that include public private partnerships and international coordination and cooperation of an unprecedented nature.
- If the problems posed by cyber security cannot be solved, the implications will be severe. There is a genuine risk that the Internet, the very essence of a globalising world, will become either dysfunctional or disintegrate into a set of separate intranets. In either case, the economic, financial, societal, political and security implications would be massive.

Moreover, cyberspace provides the ultimate environment for asymmetric warfare. Individuals or groups are attracted to the extremely low costs and the relatively low levels of technical expertise needed to conduct offensive operations against important government, economic, financial and military assets. In 2008, preceding the Russian conventional attacks on Georgia, a series of sophisticated cyber assaults disabled Georgian government, media and military assets, providing a “glimpse of the future face of war.”

2. THE RESPONSE

2.1 OVERVIEW

Policy-makers, industry leaders and experts recognize and are aware of the grave and increasing vulnerabilities of the networks upon which we depend for virtually all transactions, exchanges, critical infrastructure protection, mobility, safety, banking and business activities. In fact these software, hardware and user-related technological vulnerabilities have been the topic of serious discussion for years. Unfortunately, to date, after countless initiatives and consultations, there still has not been enough progress toward creating an effective and sustainable global system for responding to cyber-crime and cyber-threats. This is mainly due to:

- A lack of proper incentives (or liability) for technology and software producers to integrate security elements, which are essential for the protection of the consumer.
- An unrealistic expectation that the end-user is able, willing or aware enough to be responsible for the security of his/her own computer or mobile device, and therefore also of the network.
- Divergent legal systems and laws relating to cyber-crime and cyber-security; some countries have no laws relating to cyber-crime or cyber-security legislation while others have relatively advanced cyber-security frameworks. There will always be the challenge of dual criminality issues between legal systems but without, at a minimum, an international framework to "track and trace," there is little hope of catching the criminals.
- Virtually no consequences/sanctions for cyber-criminals due to the difficulties inherent in implementing legal procedures within national borders for a crime committed in a borderless world (the internet). This is made particularly difficult when many countries do not have legislation in place that even recognizes cyber-crime.
- The inability of some governments to cooperate fully due to national security priorities.
- The lack of reporting and monitoring of cyber-crimes, malware and fraud on-line.
- The challenge for developing countries to finance necessary cyber-security measures; without which the global system remains highly insecure.
- A lack of trained personnel.

The complexity of the issue makes it extremely difficult to develop an overarching effective response, which is agreeable to all stakeholders. Some, such as the ITU are calling for an international cyber-treaty, others prefer a national or a piecemeal approach defined by sector and with a focus on capacity-building. The optimal solution would no doubt involve, as is the case in other fields, a combination of international and national, legal, sectoral, public-private and end-users working together in a coordinated manner. An international framework (similar in principleto the Geneva Convention on traditional warfare) to which countries could adhere, complementing national regulatory bodies, public-private partnerships (in particular as relates to the protection of critical national infrastructure), private sector initiatives and the end-user would be optimal. Is this achievable? What about developing countries, least developed countries and failed states? Who are the key players and what kind of challenges do they face? Who needs to do what in order to achieve cyber-security?

2.2 THE KEY PLAYERS

2.2.1 Governments

Basically, states have legal, organisational, political, and leadership responsibilities in establishing cyber security. Because cyber security and protection of critical information infrastructures are so essential to a nation's security and well-being, the overall effort must be led from the highest level of government. It has to assign responsibilities and accountability, and ensure oversight and continuity of all the necessary efforts. Government has to lead a coherent response to secure the nation's advantage in cyberspace by reducing risks and exploiting opportunities through improving knowledge, capabilities, as well as decision-making. At the national level, this is a shared responsibility requiring well-coordinated action related to the prevention, preparation, response, and recovery from incidents on the part of all ministries and government agencies, the private sector and citizens. At the regional and international level, this entails cooperation and coordination with all relevant partners. And it is government that has to select the best qualified and prepared personnel to spearhead and lead these efforts.

Among the key political responsibilities of the state are: the establishment of a Cyber Security Strategy that is consistent with the overarching principles of the National Security Strategy; an associated cross-government program of work with the provision of standards, policy, and guidance on Information Assurance, information security and resilience; to ensure sufficient funding; the growth of skills and expertise needed by government, industry, and the public to secure the nation; sufficient research and development efforts as well as ensuring that these are focused, coordinated, and exploited to best effect. A further political responsibility of the state is to ensure international coordination, cooperation, and harmonization of the efforts to secure cyberspace.

Foremost among the organisational responsibilities of the state is taking all measures to effectively secure the nation's critical infrastructure and to provide appropriate response capabilities. As all levels of government now rely on cyber networks and assets to provide national security, public safety, and economic prosperity, government operations depend on IT systems that are well maintained, protected, and secured from exploitation and attack. The increasing frequency and sophistication of cyber attacks on critical infrastructure and key resources requires not only thorough planning across national, regional, and local security components, but also the establishment of new structures, organisations, and instruments to prepare for and respond to events that can degrade or destroy governments' abilities to deliver essential services to citizens, and equally to prepare for the impact of terrorist activity or natural disaster.

Challenges for Governments:

The picture of what states have achieved so far in securing their cyberspace and their critical information infrastructure varies widely. While some countries such as the UK, Australia, Canada, Finland, France, Belgium, Israel and the US have established a Cyber Security Strategy and have implemented a national framework for cyber security and critical information infrastructure protection, others are still struggling with finding a comprehensive approach.

Of particular concern, are the often meagre resources available in developing countries, least developed countries and failed states to establish and implement an effective cyber-security regime. Without the participation of all countries, the overall system remains vulnerable to attack. International cooperation is hampered by these large discrepancies between national cyber capabilities. There currently exists a "cyber abyss" between the OECD world and most parts of Africa. These discrepancies are likely to be exploited—thus exacerbating the problems of the OECD world and, in the long run, at the same time fundamentally jeopardizing the economic development prospects of Africa. In the end, with regards to cyber security, we are only as strong as the weakest link.

With few exceptions, governmental responses to the threats and risks of cyberspace have taken two tracks: legal and organisational. Neither has been very well unified or coherent, rather, they have been more organic in their development and, consequently, less cohesive than one would wish. A lack of leadership, organisational stability and expertise are the main factors limiting the capacity to respond. Some of the highest hurdles for governments exist in the legal realm, where the very nature of cyberspace is inextricably at odds with fundamental distinctions drawn in jurisprudence, such as civilian or military, foreign or domestic.

The situation is not aided by the episodic attention paid to cyber issues by legislative bodies around the world. There has been insufficient continuity in handling cyber security issues in legislatures, which address the question only in fits and starts

The legal responsibility of the state is to provide a framework for the securing of the nation's critical infrastructure and a law pertaining to crime in cyberspace. A major legal obligation of states derives from the long established principle of international law that "a state is bound to use diligence to prevent the commission within its dominions of criminal acts against another nation or its people." This principle is reflected in numerous state declarations, judicial opinions, and publications from leading scholars. It is equally clear from state practice and opinio iuris, the two bases for customary international law, that states have an affirmative duty to prevent also non-state actors within their borders from committing attacks on other states. Toleration of such attacks constitutes a crime under international law. In addition, government has to safeguard privacy and civil liberties, and to adequately harmonize data protection.

McAfee survey 2010[9]

McAfee, the world's largest security technology company, undertook a survey of 600 IT and security executives from critical infrastructure enterprises in the energy, transport, water and sewage, government, telecoms and financial sectors in fourteen countries. They all answered detailed questions about more than twenty-four different security measures—technologies, policies and procedures—and how these were used. The report paints a detailed picture of the way those charged with the defence of critical IT networks are responding to cyber attacks, attempting to secure their systems, and working with governments.

Amalgamating this data shows which countries and sectors have the highest and lowest adoption rate of security measures overall. This is not necessarily a measure of how good security is in a sector or country, but it does offer insights into security practices based on the objective rate at which key security measures are deployed. Using this measure, China has the highest security adoption rate overall (62 percent), well ahead of the US, the UK and Australia (with 50–53 percent the next highest rated countries). Italy, Spain and India have the lowest security adoption rates (all fewer than 40 percent), while Japan, Russia, France, Saudi Arabia, Mexico, Brazil and Germany are all in the 40–49 percent range. The sectors with the highest adoption rates are banking and energy, while the water and sewage sector have the lowest rate of any sector.

Critical infrastructure owners and operators worldwide report that their networks and control systems are under repeated cyber attack. The report shows that 54 percent have already suffered large scale attacks. Assaults run the gamut from massive Distributed Denial of Service Attacks (DDOS) designed to shut down systems all the way to stealthy efforts to enter networks undetected. 60 percent of those surveyed believe that foreign governments are already engaged in attacks on critical infrastructure in their country. The US (36 percent) and China (33 percent) are seen to pose the biggest threat. Other cyber attackers range from individual hackers and e-vandals to organised crime enterprises. Financially motivated attacks like extortion and theft-of-service are widespread. The impact of cyber attacks varies widely, but some of the consequences reported are severe, including critical operational failures.

The report also found that the risk of cyber attack is rising. More than a third of IT executives (37 percent) said the vulnerability of their sector has increased over the past 12 months, and two-fifths expect a major security incident in their sector within the next year. Only 20 percent think their sector is safe from serious cyber attack over the next 5 years.

The reported cost of downtime from major attacks exceeds US$ 6 million per day, but in some sectors such as oil and gas it can surpass US$ 8 million per day. Apart from cost, the most widely feared loss from attacks is damage to reputation, followed by the loss of personal information. For this reason alone, most cases of critical infrastructure cyber attacks remain unreported. Other key report findings are:

- Security is the top factor in making IT investment and policy decisions: 92 percent said security was either "vital" or "very important." Executives in China and the US were the most likely to call security "vital."
- Low confidence in preparedness: More than a third believes that their sector is unprepared to deal with major attacks or stealthy infiltrations by high-level adversaries. Saudi Arabia (90 percent), Mexico (75 percent), and India (68 percent) emerge as the least confident in preparedness, while Germany (78 percent) and the UK (64 percent) are the most confident.
- Doubts about the capabilities of governments to prevent and deter attacks: 45 percent believe their governments not very capable of preventing and deterring cyber attacks. Two-thirds in Brazil and Italy think their government incapable. Only US and Chinese respondents deem government capable.
- Doubts about the ability of their own critical infrastructure providers to offer reliable service in the event of a major cyber attack: 30 percent lack confidence that their bank or other financial service provider could offer reliable service. 30 percent have the same doubts about their telecommunication provider. Confidence in resilience is lowest in Italy, France, and Spain.
- Recession-driven cuts raising the risk: Two-thirds of IT executives claim that the current economic climate has caused cutbacks in the security resources available. Cuts are particularly evident in the energy and oil/gas sector, and are most widespread in India, Spain, France and Mexico, least in Australia.
- Laws ineffective in protecting against potential attacks: 55 percent believe that the laws in their country are inadequate in deterring potential cyber attacks, with those based in Russia, Mexico, and Brazil being the most sceptical; Germany, followed by France and the US having most faith. 45 percent do not believe the authorities capable of preventing or deterring attacks.
- Insurance firms bearing brunt of cyber attack costs: More than half of those surveyed expected insurance to pick up the cost of a cyber attack. It is interesting to note in this context that insurance practically does not exist against cyber attacks.

[9] Stewart Baker, Shaun Waterman & George Ivanov, « In the Crossfire: Critical Infrastructure in the Age of Cyber War », Report commissioned by McAfee and authored by the Center for Strategic and International Studies (CSIS), Santa Clara, CA, McAfee, Inc., 2010.

2.2.2 Legislative Bodies

Since it is necessary to establish legislative oversight over all governmental endeavours that require taxpayer funding, a great majority of states have parliamentary committees that are supposed to ensure oversight over the efforts to secure cyberspace and protection of critical national infrastructures. In some countries, these committees exercise oversight over a sector called homeland defence, while in others the committees are said to be in charge of supervising all levels of government that rely on cyber networks and IT assets to provide national security, public safety and economic prosperity. In practice, the mission and responsibilities of these committees are neither obvious nor clear. What is it exactly what these committees are supposed to oversee? Do the members of these committees have the necessary knowledge, insights, competence, and preparation for legislative oversight over a domain of such extraordinary complexity? The committees often fail to fulfil their core mission: providing legislation that keeps up with the current challenges of cyber crime. As technology evolves and new threats emerge, legislators must at least continue to ensure that cyber crime laws are modernized to match these threats.

Challenges for legislative bodies:

- The technical complexity of the issue, which surpasses the professional experience of most members of parliament and requires highly specialized staffers that few parliaments can afford.
- The fact that cyber security is a cross-cutting issue, which cannot easily be fitted into existing committee structures. To put it simply: Who is in charge—the armed forces committee or the security committee? Justice, police, or the committee for homeland security? Telecommunications? Or all of them? And what role is there for Foreign Affairs?
- Few countries have adopted a 'Cyber Strategy.' What should therefore be the yardstick against which performance in this area should be measured?
- Cyber security is addressed, fully or partially, by many countries through their military and/or intelligence structures—i.e. through agencies that are, by their very nature, more exclusive and non-transparent.
- Even the most fundamental task of a parliament, namely to unequivocally determine that the country has been subjected to a foreign military attack and therefore is at war, is—more likely than not—beyond the capacity of most parliaments today. There is no clear definition of what constitutes a cyber-attack. In addition, attackers hide—in a world where a country is not responsible for any cyber activities of its citizens—behind anonymous alleged private 'hackers' and 'hacktivists.' This makes countries vulnerable, particularly in the developing world, and constitutes a challenge to the very basis of international order and peace.

New, more professional and efficient ways and means may be needed to assist parliament in this particularly demanding task to cope with the complex problems of oversight over all measures related to the prevention, preparation, response, and recovery from cyber incidents on the part of all ministries, government agencies, and the private sector. The greatest need is to improve mutual assistance and international cooperation on cyber crime among governments, industry, and NGOs. And there is a need to provide technical, business process and policy advice to leaders in both the executive and legislative branches of government as they help tackle the challenge of securing cyberspace and protecting critical infrastructure. Close cooperation with critical infrastructure industries is required to helping both government and industry understand the value of public private partnerships, and the necessary steps that must be taken to ensure that infrastructures are sound. Government must be supported on all aspects of securing cyberspace. And a cross-government as well as cross-agency perspective must be encouraged.

2.2.3 The armed forces

The armed forces have to constantly reckon with the fact that the security of their networks, IT systems, and communications could be breached, and their systems infected, manipulated, disrupted or destroyed by cyber warfare. Malicious code could spread undetected, establishing digital beachheads from which data could be transferred to servers under foreign control, delivering classified information to unknown adversaries.

IT technology and the digital infrastructure enable almost everything the armed forces do: command and control of forces; real-time provision of intelligence, reconnaissance, surveillance and targeting information; planning and operations; logistical support; and administration. While reliance on these means can provide military forces with critical advantages over adversaries, it can also enable adversaries to gain knowledge about intentions and capabilities in order to impede or disrupt operations.

Since cyber warfare is asymmetric, and cyber warfare devices are cheap, adversaries do not need to build expensive weapons and develop traditional armed forces to pose a significant threat. A small number of determined computer programmers can, if they find a vulnerability to exploit, gain the knowledge to threaten national armed forces, steal operational plans, blind intelligence capabilities, hinder the ability to deliver weapons on target, or disrupt logistics. This is why many militaries are developing cyberspace offensive capabilities.

However, the problem for countries with advanced militaries is that while they have offensive cyber capabilities, so do their opponents, against whom they must defend. In the nuclear era, a strong offensive capability could serve a defensive purpose, by threatening retaliation and thus deterring an opponent from attacking. Applying this deterrent formula to cyber conflict seems logical, but the notion of cyber deterrence is deeply flawed. In cyberspace, no one can be confident of their ability to determine an attacker's identity. Sophisticated attackers are skilled not only at hiding their identity but also making it look as if someone else was responsible. The scope of collateral damage is also difficult to predict, including both unintended effects on the target and damage to third party networks connected to or dependent upon the target network.

While uncertainty and confusion have always been part of warfare, the fog of war is especially thick in cyberspace. And the implications of uncertainty are most pronounced for deterrence. Deterrence depends on the threat of retaliation to change the opponent's calculus of the benefits and cost of an attack. But not only is it hard to convincingly threaten an unknown attacker, the context for deterrence has also changed. There was symmetry in vulnerabilities in the Cold War. That symmetry no longer exists. Advanced nations are more dependent on digital networks and this asymmetric vulnerability means that even in an equal "exchange" of cyber attacks, one side will lose more than the other. Furthermore, an anonymous attacker may not lose anything since his identity is unknown and retaliation is impossible.

Particularly non-state opponents are much less likely than states to be deterred by the threat of retaliatory attack. And their willingness to accept risk will likely be much greater than most states since they have no capital city, infrastructure or assets to threaten. In addition, they do not face the same political constraints that apply to state action in cyberspace. Some may even welcome retaliation, as it could provide justification and expand support for their cause. The best evidence of the weakness of deterrence in cyberspace comes from the US, which has some of the most advanced cyber offensive capabilities in the world but obtains no deterrent effect from them.[10] Thus, while nuclear weapons deterred a potential aggressor, cyber weapons do not.

Challenges for the armed forces:

- The military has become completely dependent on cyberspace for its activities. Any threat in the cyber domain is of fundamental consequence for the armed forces.
- The revolution in military affairs has, by focusing on robotics and precision delivery of kinetic energy, rendered the military increasingly vulnerable to cyber attacks.
- The traditional conservatism of the military is a hindrance (historical examples include the difficulties that militaries have had with the introduction of the machine gun, the dreadnought, the tank, or aircraft carrier). There is some truth in the saying that the military always tends to prepare for the last war.
- Cyber power has not yet been massively demonstrated. Most cyber threats today are the product of individual perpetrators or relatively small, organised criminal groups. The true military potential of cyber, if yielded as a weapon by a cyber advanced country, has only been hinted at in the cases of Estonia and Georgia, and more forcefully, by the recent "Stuxnet" attack on Iran.
- Stuxnet is said to be the first direct example of weaponized software that targets industrial control systems, designed to cause physical harm to systems outside a computer or computing network, thus heralding a new era in cyber war.
- Cyber defence on a large scale requires cooperation between the private sector and the military
- Should cyber indeed replace kinetics as the prime manifestation of military power, the repercussions for the mission, the strategic and logistical conduct of operations, the structure, the equipment and the very nature of armed forces would be significant.
- Cyber advances will have a serious impact on the relative military strength of nations and the international balance of power
- Cyberspace presents the military with questions for which there are not only no answers, but for which we might not even have understood the questions yet.

[10] See among other publications: The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, TRADOC Pamphlet 525-7-8, Department of the Army, 22 February 2010.

Broad improvement in cyber security internationally will require nations to undertake a larger strategic calculation to determine the balance among offensive, defensive and multilateral efforts that best reduce the risk and increase the cost of cyber attack. Most nations have not done this yet. The notion of cyber deterrence is appealing because it is unilateral and justifies building offensive capabilities. But real security may require exactly the opposite approach—multilateral agreements and emphasis on defence.

2.2.4 Law enforcement

Mirroring the international openness of the Internet, cyber crime is to a large degree transnational in nature. Perpetrators and victims are frequently located in different jurisdictions, which poses acute difficulties for law enforcement agencies in investigating and prosecuting online crimes. Despite the need for international cooperation on cyber crime, there is as yet no genuinely global multilateral treaty dealing with the issue. Issues of national sovereignty can impede criminal investigations and cooperation between the law enforcement agencies of the jurisdictions involved. The speed at which cyber criminals can inflict harm and evade detection puts enforcement agencies under heavy time pressures, making the need for international cooperation all the more pressing.

Legislative convergence is crucial to effective cooperation. This is because many countries base mutual legal assistance on the principle of dual criminality, which requires that the offence in question be punishable in both jurisdictions. Where a particular jurisdiction lacks comprehensive cyber crime legislation or enforces it poorly, it may turn into a safe haven for cyber criminals. This kind of divergence can only be tackled by concerted efforts to harmonize legal standards and by enhanced cooperation.

Law enforcement cooperation in combating cyber crime is not only hampered by a general lack of skilled manpower and financial resources; cooperation is seriously deficient because cyber crimes are still dealt with by basic police structures. These entities lack expertise, responsiveness, and clear techniques and procedures for responding to cyber crimes. Insufficient cyber forensics personnel, numerous barriers to cooperation, outdated or nonexistent legal remedies, paucity of cross-border cooperation, and individual organisations' cultural paradigms prevent the implementation of effective solutions.

The response to criminal activity in the physical world is hard to replicate in cyberspace. Yet this merely highlights the necessity for comprehensive cyber crime statutes with harmonized, substantial, and severe sentences. Even cases with an incontestable chain of evidence all too often fail to result in incarceration. One of the notable outcomes from the few successful cases is the unprecedented demonstration of how multiple international law enforcement agencies can work together, share information and techniques to gather evidence, identify the perpetrators, and arrest them. However, such a level of collaboration is the exception rather than the rule.

Challenges for law enforcement:

- While Internet criminality is international in nature, cyber crime legislation varies from country to country.
- Even in advanced countries, the evolution of the threat far outpaces the necessary adaptation of the penal code and other basic legal texts.
- Cyber crime is often international—for example, a child pornography site may be registered in country A, be produced in country B, and owned and controlled by a citizen of country C. The same applies to the production, and use, of malware.
- A country is, under international law, not responsible for the cyber activities of its citizens, even if those activities constitute de facto the equivalent of an act of war against another country. The situation invites cyber ambitious countries to hide their own cyber activities behind the cover of allegedly anonymous hackers or hacktivists.
- The misuse of computers may become apparent only after time, when Trojans or other delayed action malware is activated. It may also be difficult to detect (for example, if malware steals 5 cents from every money transfer between country A and country B).
- Some victims of cyber crime my not want to call in the police, for example, banks who, probably rightly, assume that the damage caused by the theft becoming public might outstrip the losses incurred due to the crime. At a larger level, this creates a situation in which an increasing sector of the economy is silently slipping from the protection of the law, and has to rely for its protection on its own devices and/or specialized private companies.
- In most countries, the number of cyber police officers employed is small and career prospects are correspondingly limited. Police forces are hard pressed to compete for the best and brightest with the private sector.
- With their own devices, police forces are not able to detect most forms of cyber crime, but have to rely both for the detection and the prosecution of such crimes on private companies such as Internet service providers, mobile phone operators, and other specialized agents. The police are, in one of the most quickly evolving areas of criminal activities, no longer able to guarantee security to its citizens through its own devices.
- This leads to a situation in which the police are no longer held responsible for cyber security. And where there is no responsibility, there is no accountability. This, in turn, renders the development of functioning cyber security approaches and strategies all the more difficult.

Perceived deficiencies contribute to the fact that targets of cyber crime may not believe that law enforcement agencies will be able to identify offenders.[11] The first point of contact for a victim of cyber-crime is the local police station, which is generally unequipped to deal with the issue and do not feel responsible for solving the crime. Fault is generally pushed onto the internet service provider, the payment system or the website where the problem may have occurred, forcing the responsibility back onto the victim. Comparing the large number of cyber crimes with the few successful investigations, victims also see little point in reporting offences. Moreover, automation means that cyber criminals follow a strategy of reaping large profits from many

[11] Russell G. Smith, "Investigating Cyber crime: Barriers and Solutions", Pacific Rim Fraud Conference, 2003, p. 2.

smaller attacks. But for only small amounts, victims may prefer not to go through time-consuming reporting procedures.[12]

One of law enforcement's biggest problems is the recruiting and retention of personnel highly qualified in cyber security and cyber forensics. Government service remains unattractive as long as it cannot compete with the salaries, career opportunities, and training prospects offered by the private sector. Government needs a strategy to expand, improve, train and retain a technologically advanced IT workforce.

While many law enforcement agencies are technically adept and eager to investigate online and cyber crime, they find a paucity of support from prosecutors, judges, and policymakers. Law enforcement needs greater support from these entities, as well as from systems of improved global collaboration.

2.2.5 Judges and prosecutors

While in many countries, law enforcement authorities have been able to strengthen their capacities to investigate cyber crime and secure electronic evidence, this has been less the case for judges and prosecutors. Experience shows that in most cases, judges and prosecutors encounter difficulties in coping with the new realities of the cyber world. Particular efforts are therefore required to enable judges and prosecutors to prosecute and adjudicate cyber crime, and to make proper use of electronic evidence through training, networking and specialization.

The expertise of the private sector with respect to new technologies has been essential for law enforcement training. It will also be beneficial for judicial training, but this potential has so far been underused. At the same time, the independence and impartiality of judges and prosecutors must be maintained. All judges, investigative judges and prosecutors should have basic knowledge of matters related to cyber crime and electronic evidence. They should be able to understand computers and networks, how information and communication technologies are used to commit crime, domestic legislation and international standards, jurisdiction and territorial competencies, and technical procedures as well as legal considerations in securing electronic evidence.

As a result of such training, judges and prosecutors should be in a position to relate criminal conduct to provisions in domestic legislation, approve investigative techniques, order the search and seizure of computer systems and the production of electronic evidence, expedite international cooperation, question witnesses and experts, and present and validate electronic evidence. However, sometimes basic knowledge is not sufficient to carry a judicial case of cyber crime. To face such situations, investigative judges and prosecutors with advanced knowledge are needed

[12] Serious Organised Crime Agency (SOCA); "International crackdown on mass marketing fraud revealed", 4 October 2007.

to investigate, prosecute and judge complex cyber crime cases, or to provide support to other prosecutors and judges.

Industry must work with law enforcement, judges, and prosecutors to help develop the tools that are needed to pursue cyber criminals. Internet service providers, bankers, financial service providers, money transfer agents, law enforcement, judges and prosecutors must be engaged at the same table to ensure the improved tracking of cyber criminals, a better understanding of their methods, and ultimately the gathering of forensics evidence in a timely fashion. Internet service providers, in particular, should be actively engaged as part of the solution, given their important oversight and responsibility for the Internet traffic, which flows through their networks.

Challenges for judges and prosecutors:

- The global nature of cyber crime makes arresting and prosecuting cyber criminals difficult.
- Cyber crime laws are not up-to-date, contain loopholes or do not exist at all; penalties for cyber crimes are weak; many impediments exist for investigators in forensics search and seizure and in obtaining witness cooperation.
- There is an urgent need to ensure that all countries have in place strong and harmonized legal frameworks for cyber crime
- Judges, prosecutors and law enforcement agencies often lack sufficient knowledge to effectively bring cyber criminals to justice. More must be done in training and education to ensure that these officials have the knowledge, skills, and capacity to properly fight cyber crime and to make their charges stick.
- The cross-border sophistication in tracking and arresting cyber criminals needs to be improved
- Governments, internet service providers, financial services providers, banks, money transfer agents, communications and mobile phone operators and security experts must be engaged across borders and encouraged to work together.

Although the perpetrators are still well ahead of the law makers, the EU is trying to catch up as cyber crime increasingly threatens data protection of citizens, industry and government services. National action has proved inadequate to tackle the growth in online banking fraud and identity theft, phishing of social network accounts, computer-crippling viruses and the sale of illicit pornographic content. EU member states now admit that collaboration is needed at the European and international level to deal with the problem.

Some progress has also been made regarding the training of judges and prosecutors. In July 2007, Europol set up the Cyber Crime Investigation Training Harmonization Group, which has the primary objective of coordinating the efforts within the EU on high tech crime training. This will help to establish a certified training curriculum for law enforcement investigators within Europe, and to disseminate this beyond the EU. Partners include the European Commission, the European Anti-Fraud Office OLAF, Eurojust, the European Police College CEPOL, Interpol, Council of Europe, United Nations, UCD Centre for Cyber crime Investigation – Europe's leading centre for research and education in cyber crime and digital forensics, University of Troyes, Canterbury Christchurch University, University of Bologna, as well as the private sector. Member states on 27 April asked the Commission to look into setting up a special agency to tackle cyber crime "to evaluate and monitor the preventative and investigative measures" that member states should carry out.[13]

2.2.6 The End User

There is great need for IT user awareness and education. All users, including consumers, small businesses, children, schools and company employees must be aware of the risks of cyber crime, as well as of the best practices required to protect themselves. Education and awareness initiatives should be launched and a cyber security curriculum should be created that could be used not only in schools, but also through all sorts of youth organisations, crime prevention associations, neighbourhood watch associations and groups engaged in consumer protection.

Would-be criminals need to understand that they do risk getting caught and that cyber crime is as serious as crimes with a "face." Advertisers also need to be aware and ensure that their legitimate expenses for advertising do not end up funding some illicit activity. Work must also continue with commercial actors to ensure they have are engaged in ensuring the security of their knowledge assets—their data—and their businesses.

The public at large needs to become more aware that an attack on critical infrastructure can cause loss of life, threaten public safety, impact national security, cause widespread economic upheaval, or create devastating environmental disasters. More must also be done to raise public awareness on the critical importance of reporting all electronic intrusions and associated losses to law enforcement. This way the public can help to ensure law enforcement officials have the knowledge, skills and capacity to properly fight cyber crime and that laws are improved to better penalise criminals.

2.2.7 The Private Sector

If the government response to cyber security can be characterized as ad hoc, the private sector response to cyber security can best be characterised as unstructured. There are three traditional responses to market failures of this sort: regulation, taxation and insurance pricing. Insurance pricing is not feasible without both standards against which to measure conduct and liability that arises from failure to meet those standards.

[13] Council of the European Union, Council conclusion concerning an Action Plan to implement the concerted strategy to combat cyber crime, 3010th General Affairs Council meeting, Luxembourg, 26 April 2010.

In the cyber domain, neither is readily available. There are no generally accepted cyber security standards, and there is no generally applicable liability system in place to account for failures to meet those standards. The relevant insurance question is: how to underwrite the risk? And the answer only can come if the risk-taker is motivated by liability to insure the risk in the first place. Such a system does not exist.

Creating incentives for security in the private sector cyber domain remains a challenge. For a host of reasons, private sector companies are unwilling to publicly identify security risks and equally unwilling to voluntarily create standards that lead to liability where none currently exist. If the government does not step in to set standards for the private sector to follow, then none are likely to be developed. But the construct of a government-developed set of standards is itself fraught with challenges. One alternative is to reverse the paradigm: instead of government creating standards, the breach of which might result in liability, it might be more feasible for government, in partnership with industry, to develop a set of recommended best practices for cyber security. If it did so, it is possible that an independent certification industry would develop, and that insurance rates would follow compliance with those standards. Alternatively, though less efficiently, the government might itself give a "seal of approval" and certify compliance with the best practices standards. In either event, if standards could be developed, then insurance against the risk of breach of those standards would naturally follow.

A more intrusive step would be to change from advisory standards to a traditional regulatory model of mandatory standards. This, too, would raise questions about government's ability to define the standards appropriately. It would, moreover, raise the routine problem of how to make regulatory mandates operational in a complex technical area. However, it may also be that the regulatory model can be followed without any standard-setting. All government need to do is define the desired outcome—for example, appropriate reductions in data breaches or intrusions—and define the penalties for failure. Simply creating consequences also creates liability (and thus insurable risk) even in the absence of a mandate on how to achieve the results desired. As long as the desired results expressed are not impossibilities—such as elimination of all intrusions—this would leave the private sector to determine the most cost-efficient means of achieving the public policy objective. But there are not enough real incentives for the private sector to do so.

The final means by which government can create incentives for private sector activity is the tax code. Taxing an output, or by providing a tax credit/incentive for expenditure, a financial incentive to act could be created. Though this can also have unintended or undesirable consequences, taxing remains a tool by which governments have frequently sought to modify private actor conduct. In this case, for example, parliament might consider a tax credit for qualifying expenditures on security systems as a way of pushing the private sector towards more security-conscious decisions. This would require some confidence in the government's ability to craft the right incentives. And this is precisely the problem. Especially in the cyber domain, where private sector actors are notoriously distrustful of government interference and regulation, it will take a significant effort of political will to create a culture where civil law drives security reform.

2.2.8 The IT Sector

The IT sector is a critical part of any cyber-security solution and, as cyber-threats and attacks increase, may even slowly replace the traditional security sector as the lynchpin of national defence strategy. This will bring with it a range of challenges, in particular perhaps for the industry itself—how to retain an independent, free-thinking, innovative nature while also playing a central role on national security issues?

In the short term, the IT sector must be encouraged to help provide technology solutions that stay one step ahead of the threats. It must work together to accelerate the development of interoperable security products, and simplify the integration of these products with complex customer environments, with the aim of both securing the network and ensuring availability of critical assets.

The quality of software also needs to improve. Much attention has been on operating system security, but the target has now moved to the application layer, which has had insufficient security focus. Beyond the application layer, lower level software such as firmware is poised to be the next target of attack. There has been little to no attention aimed at reducing the vulnerabilities in this space, which must change.

Security must become easier or built-in. The more difficult security is, the less people will use it. Relying on the end-user to be responsible for the security of his/her PC or mobile device is perhaps akin to asking a car driver to purchase his/her own airbag or seatbelt as an "extra" for protection in case of accident. Perhaps private sector companies should be held responsible or made liable to some extent for damages caused by insecure IT products and services.

Internet domain registration needs to become scam proof. In the area of critical infrastructure protection, greater dialogue is necessary between those producing solutions and those implementing. This ensures the right solutions, with a focus on the availability of the network, and accounting for special considerations that must be a factor in the use of commercial solutions.[14]

Technology companies must partner with each other, businesses, academia, government, and think tanks to fully understand the new threats and benefit from the latest academic research. A research coalition among customers, law enforcement,

[14] McAfee, "Multipoint Strategy to Fight Cyber crime," 30 November 2009.

Internet service providers, banks, mobile phone operators and other stakeholders should be encouraged.

2.2.9 Banks and financial services

The volume and variety of electronic financial services have increased significantly, and the use of the electronic medium to do business, whether online or through remote mechanisms, has spread rapidly over the past two decades. Since the mid-1990s, investment in banking technology has focused on online banking, brokerage, and insurance services to increase convenience, improve quality of service and to reduce costs. Emerging markets increasingly use new methods of e-payment and wireless technology for e-finance. But with the benefits of new technology also come new and virulent risks of fraud, theft, extortion, credit quality deterioration as well as systemic risk. Financial services and the payment system in particular, constitute one of the most important areas of critical national infrastructure. A compromised payment system caused by illegal access or hacking would have broad ramifications for the entire economy. Public interest and welfare are potentially at risk when business and commerce fail to meet certain minimum electronic security standards.

A major problem with banks, financial services, and some other private enterprises is their reluctance to report electronic intrusions to law enforcement. They often find it easier to keep quiet and absorb the pain inflicted by attacks and intrusions, even at substantial cost. There are five reasons banks or financial service providers are hesitant to report intrusions and losses to law enforcement: (1) negative publicity, which could convert their vulnerability into a stock valuation problem, jeopardize their market position, strategies, customer and public confidence, or capital investments; (2) negative information competitors would use to their advantage, for example, by customer poaching or piracy; (3) the need to protect individual customer's privacy; (4) the risk of exposing themselves to costly and time-consuming litigation; and (5) fear among IT personnel of reporting incidents due to worries about job security. In addition, there might be a lack of trust towards law enforcement, or a concern that reporting may lead to increased regulation of the industry or of e-commerce in general.

However, continued indulgence of such behaviour is creating a most problematic and dangerous situation. If government is incapable to impose compulsory reporting of intrusions and losses by banks and financial services, it will deprive the state of its monopoly of the use of force necessary to enforce the rule of law. It will also have a direct impact on another important obligation of banks and other financial services: the prevention, and reporting of money laundering. Government and all authorities engaged in the fight against cyber crime must impose compulsory reporting by all victims of cyber crime. Access to more precise information about the true incidence of cyber crime would also enable law enforcement agencies to better prosecute offenders, deter potential attacks, and enact more appropriate and effective legislation.

Challenges for the banks:

- Due to the massive amount of money being transferred electronically around the globe every second, financially motivated cyber criminality is on the rise.
- The situation is rendered even more attractive for criminals by the fact that banks, more often than not, do not report successful attacks.
- There is no insurance available for cyber burglary (there is no "community of victims" large enough to render such insurance profitable and, equally important, calculable).
- There is, in most countries, no cyber branch of the police force. Moreover, cyber police forces around the world tend to specialize in a few areas (such as pedophiles or human trafficking).
- Banks are not only the victims of cyber burglary, but of a whole range of criminal attacks—from attempts to unlock client data to money laundering.
- In the case of central banks, the potential objectives of cyber crime multiply and include access to sensitive data of all kinds—from decisions on interest rates to planned interventions in money markets.
- Confronted with this evolving reality, the banking sector counts increasingly on its own defences, ranging from in-house capabilities to expensive, and highly selective, outside assistance.
- In the banking sector, there is a net trend to no longer count on any meaningful support from the forces of law and order. This is a quite extraordinary situation—for the banking sector accounts in some countries for a significant percentage of the GNP and is, in all countries, the life blood of a functioning economy.
- This situation is untenable in the medium and longer term. If the banks cannot count on their cyber integrity to be defended by the state and the international community, the financial sector will ultimately opt for highly classified intranet solutions—a step that would have profound implications for the world economy in a globalising world.

2.2.10 Critical National Infrastructure

Protecting critical national assets and services in an increasingly complex and unpredictable inter-connected world is becoming ever more difficult. A nation's defence, public safety, the economy and the quality of its national life have long depended on the efficient delivery of a number of essential services, among them telecommunications, energy, banking and finance, transportation, and vital human services such as the provision of food and water, and emergency response services. These national essential services have, over time, become known as Critical National Infrastructure (CNI).

The rapid growth and integration of a worldwide telecommunications infrastructure, based largely on the Internet, has brought critical infrastructures together in a manner, which was hitherto unimaginable. Tracking dependencies has become complicated and elusive, in particular when critical infrastructures straddle the private and public sectors.

Addressing the challenges of securing cyberspace requires a coordinated response that unites internal, foreign and defence policy. The EU thinks that the OSCE's unique cross-dimensional approach to security can provide an excellent foundation to meet this challenge. But as of yet, there seems to be no single answer or approach throughout the EU. The fact that CNI such as energy, telecommunications, transport and water in Europe are becoming increasingly interdependent, creates more complexity, and raises the risk of severe disruptions.

Currently, the understanding of the pan-European CNIs with their broad range of geographic and sector-specific dependencies and interaction is still underdeveloped. Studying these complex infrastructure systems demands joint interdisciplinary efforts by researchers, industrial stakeholders, and governmental organisations. This research depends on the use of models and simulation environments as a tool because disruptions and mitigating measures, for obvious reasons, cannot be studied or tested in real world circumstances.[15]

The challenges of protecting critical national infrastructures:

- The economic, financial, governmental, societal and health infrastructures of all states depend today on a functioning cyberspace. They are, correspondingly, vulnerable and attractive targets.
- The protection of CNI, has been recognized by most countries, as a priority. This basic awareness alone does, however, not translate into effective mechanisms for actual protection.
- Every sector of public and private life is today a potential target for criminal cyber attacks—and even more so for covert probing, intelligence gathering or sabotage operations by foreign powers. The state is, in most cases, not able to provide credible protection against such attacks.
- To create a genuine private public partnership in protection of CNI, the private sector would have to perceive a clear-cut, measurable advantage in reporting to law enforcement agencies, and to subsequently develop together with them a coherent defensive system. Currently, it does not.
- This renders attacks against private critical infrastructure particularly interesting: for bank robbers to terrorists to foreign powers eager to exercise their cyberwar capabilities.
- Some infrastructure is particularly critical: major airports, air traffic control systems, key nodes of the electric power grid, chemical facilities and the international financial system. These potential targets are keenly aware of their vulnerabilities, but prefer to erect their own cyber defences. A situation in which the most important and most likely targets essentially have to fend for themselves is simply not sustainable.
- The problem is exacerbated by the fact that, as examples prove, cyber malware has already been planted into some of the world's critical infrastructure systems. The corresponding need to develop intelligent systems able to check automatically and regularly for the presence of highly sophisticated malware, is only about to be understood. It will be a costly enterprise in the best of circumstances and likely to be unevenly applied, thus reducing the eventual positive effects of select countermeasures for the overall system of interlinked critical infrastructures.
- Comprehensively coherent and harmonized national approaches are indispensable in this domain; without international coordination no progress will be possible.

The initial call for member states to cooperate in infrastructure protection came in the aftermath of the Madrid terrorist bombings, where deficiencies were seen in the sharing of intelligence on the threats to CNI. Currently, there are proposals before the EU Commission whereby member states would be required to identify and designate all critical infrastructure components and undertake periodic security reviews. The

[15] See: DIESIS: Design of an Interoperable European federated Simulation network for critical InfraStructures, Fraunhofer IAIS, at: http://www.iais.fraunhofer.de/4819.html?&L=1 and www.diesis-project.eu

result of these reviews would be coordinated by a central EU coordinating body which, in turn, would prescribe and monitor standards.

However, attempting to standardize across the EU may likely be fraught with difficulty. There are 27 member states, each presumably with a particular definition of CNI, perceiving differing levels of risks and having different military, technical and political resources to meet risks and to defend against them. Thus, it may be probable that an EU-wide approach will need a degree of cooperation and information sharing beyond what is currently acceptable to individual member states, since there are already inevitable concerns about sharing such sensitive national information.

2.2.11 WikiLeaks

On 22 October 2010, the global online whistleblower, WikiLeaks.org, (according to its website "a non-profit media organization dedicated to bringing important news and information to the public") leaked 391,832 classified reports covering the wars in Iraq and Afghanistan from 2004 to 2009—the War Logs. The documents are mostly raw field reports filed by the US military, the bulk of which, some 97 percent, are classified at the secret level. WikiLeaks released the documents to a number of news outlets for analysis several weeks in advance of their formal public release. These included The New York Times, Der Spiegel, The Guardian and Al Jazeera, each of which published special reports. The Pentagon has denounced the release of the information, which it considers a crime. It has also demanded the return of its stolen property, and warned that the documents place Iraqis at risk of retaliation, and also risk the lives of US troops from terrorist groups that are mining the documents for operational information they can use in planning their attacks.

The documents contain very few true secrets, a point emphasized by the media outlets after intense research. They highlight a number of issues that had been well-known and chronicled for years, for example: that the Iraqi government was torturing its own people; that sectarian death squads were operating inside Iraq; and that the Iranian government was funding Shiite militias. None of this is news. The reports discussed things units encountered, such as Improvised Explosive Device (IED) attacks, ambushes, murdered civilians, friendly-fire incidents, traffic accidents, and so forth. For the most part, the reports contained raw information and not vetted, processed intelligence. They also did not contain information resulting from intelligence-collection operations and therefore did not reveal sensitive sources and methods. Although the material is often compared to the 1971 release of Daniel Ellsberg's Pentagon Papers, there is little similarity. These consisted of a top secret-level study of the Vietnam War completed for the US Secretary of Defense, and not raw, low-level battlefield reports. The papers showed that the government had been lying about the war and their publication was a factor in continuing to turn public opinion against it.

However, on 28 November 2010, WikiLeaks announced that it had published 251,287 US embassy cables, billing it as "the largest set of confidential documents ever to be released into the public domain." Its website claimed that this would provide an unprecedented level of scrutiny into US foreign policy. On the face of it, this would have been a researcher's dream come true. News desk journalists of the New York Times, the Guardian, Der Spiegel, El Pays, and Le Monde combing the rich trove of "virtues of diplomatic confidentially," "limited honesty in policy," and backroom deals, published a portion of the documents they received, and will release the rest gradually over the following months as other news media begin to pick them up. As was the case with the War Logs, these embassy cables were taken from the US government's Secret Internet Protocol Router Network (SIPRNet), a network used to distribute classified information at the secret level and below. The large batches of documents were released by a soldier, PFC Bradley Manning, who was arrested in May 2010 in Iraq by the US Army Criminal Investigations Command and charged with transferring thousands of classified documents and transmitting them to an unauthorized person. Manning knew the information he was downloading was classified and needed to be protected. Since he also knew that his actions were illegal and could get him in trouble, he deserves to face the legal consequences of his actions. The regulations by which information is classified by the US government are outlined in Executive Order 13526. Under this order, secret is the second-highest level of classification and applies to information that, if released, would be reasonably expected to cause serious damage to US national security.

Calling this release "cablegate," WikiLeaks claims that these documents will be a huge embarrassment to the US government, but that all contain public information that American citizens and the global community have a right to know. "The documents released reveal the contradictions between the US's public persona and what it says behind closed doors—and shows that if citizens in a democracy want their governments to reflect their wishes, they should ask to see what's going on behind the scenes." What is now circulated by the media worldwide on the Internet, TV and newspapers, is the most cardinal breach of trust and betrayal of confidence. Some of the cables defamed world leaders; others unveiled secret NATO plans for a US-led war against Russia over the Baltic States in the event of any Russian incursion. Some of the more volatile cables released include Arab leaders in the Gulf imploring the US government to take action against Iran's suspected nuclear weapons programme. Cables from Islamabad reported that the Pakistani government was again dragging its feet on an agreement reached two years earlier to allow America to remove highly enriched uranium (which was given by the US in the 1960s under the atoms for peace programme). Pakistan was afraid that, if leaked, the people and media will create an impression that the US is planning to take control of its nuclear weapons. Another cable reported the Army Chief of Staff telling the US ambassador that he might, however reluctantly, pressure President Zardari to resign and possibly leave the country. America and many of its allies are naturally embarrassed.

Future challenges: WikiLeaks

- WikiLeaks has published classified documents in spectacular fashion. In doing so, it has captured the world's attention. In itself, that is nothing new. The "Pentagon Papers" spring to mind.
- What is new, however, is first the number of documents leaked (well above 640,000). Second, it was not an individual who disclosed to someone else a perhaps large, but ultimately limited amount of documents (a KGB agent who compromised classified information; a disaffected bank employee who sold a CD with confidential clients' data to a third party; a disaffected government employee disclosing "hot" information to a newspaper). The WikiLeaks case is quite different: An Internet platform dedicated to the disclosure of private/classified information and open to all. WikiLeaks is an invitation to all to disclose any information that may disturb. The concept ranges potentially from strategic information through confidential private data to trivial stuff for Internet paparazzi.
- There are, in the end, neither boundaries nor limits to the sort of concept represented by WikiLeaks. The well orchestrated launch of the platform (a first burst of more than 390,000 war documents, followed by another large diplomatic disclosure, the whole well embedded in international media coverage) appealed to everybody, particularly the disgruntled and the idealistic, to disclose whatever dirty secret should be exposed to public scrutiny—showing people that nothing is truly secret or hidden anymore. WikiLeaks must be understood as an invitation to eliminate any secrecy—yet ultimately also any privacy.
- WikiLeaks was, however, more than that. There was, on the one hand, a previously established relationship with powerful media (from Spiegel.online to The New York Times) that promised that journalists would sift though the tons of disclosed documents in order to find the truly juicy stuff. WikiLeaks was, thus, a highly commercial enterprise. On the other hand, WikiLeaks appealed at the same time openly to, and triggered a reaction by, the anarchic, proto-democratic section of the Internet. It thus combined the high commercial with the anarchic end of the net.
- Nobody was—or still is—prepared. The phenomenon is simply posing too many questions at the same time. There is, first, the obvious question of the right of the public to know versus the right to secrecy. There are, however, much more concrete questions as well: how to protect governments (or indeed any Internet actor) from massive leaks through disgruntled personnel or any other person (such as a divorcing spouse)? How to protect—even at the private level (from Facebook to badly protected smartphones and PCs)—confidential, personal, and private data? How to handle the issue in the integrated fashion at the national level? And since that level will clearly not suffice in the age of a global Internet: What international action is needed and appropriate?
- The question is time-urgent—for if convincing and coherent answers are not found quickly and in a convincing way, the anarchic reaction to the WikiLeaks drama will transform itself into a permanent and dangerous phenomenon. It would greatly contribute to the trend to "balkanise" the internet into a large number of highly secured intranets. The consequences would be massive.

The US government, according to the US Attorney General, is planning criminal prosecution against WikiLeaks, saying that the latest disclosures of sensitive State Department documents have jeopardized the security of the nation. The Pentagon is tightening access to information, including restricting the use of computer storage devices such as CDs and flash drives. But there is no doubt that the US government is responsible for the WikiLeaks fiasco due to its laxity in protecting highly sensitive dispatches by its ambassadors. Meanwhile, Hilary Clinton and other officials have been working hard to apologize to world leaders and ambassadors in order to avoid as much backlash as possible.

WikiLeaks.org has been closed down by Amazon's managed hosting service but the action taken by big business to silence the website has caused a huge number of online retaliation attacks from free-speech activists—attacks which even downed secure payment provider Mastercard and Visa. It seems that business connectivity security will remain in the spotlight for some time as the so-called "hacktivists" announce that other sites will be hit with denial-of-service-attacks. PayPal was hit with a major, malware-led attack after it blocked online donations on the WikiLeaks website. This raises a new issue: the cooperation of internet service providers with the government. Is it censorship by another name? Or is it a business responsibility in tackling the anarchic lawlessness of the World Wide Web?

2.3 THE RESPONSE: PUBLIC-PRIVATE PARTNERSHIPS

Examples of non-binding public-private partnerships under the auspices of the International Telecommunications Union:

The ITU, as a result of the World Summit on the Information Society (WSIS) in Geneva in 2003, was mandated to lead the coordination of international efforts on cybersecurity. Specifically, the ITU was designated the organization responsible for implementing Action Line C5 of the WSIS Geneva Plan of Action: "Building confidence and security in the use of ICTs". The ITU subsequently launched the multi-stakeholder Global Cybersecurity Agenda (GCA) , within which the Child Online Protection initiative and a partnership with the International Multilateral Partnership Against Cyber Threats (IMPACT), Malaysia were established.

Key Objectives of Child Online Protection are to identify risks and vulnerabilities to children in cyberspace; create awareness; develop practical tools to help minimize risk and share knowledge and experience.[16]

IMPACT's goal is to enhance the global community's capacity to prevent, defend and respond to cyber threats.[17] IMPACT's Global Response Centre (GRC) has developed a Network Early Warning System (NEWS) and an Electronically Secure Collaboration Application Platform for Experts (ESCAPE) in collaboration with the private sector and governments. IMPACT also provides high-level briefings, global best practices, security certification and security audits.

Since a nation's cyber and critical infrastructures are to a large part owned by the private sector, a partnership of government, corporate and private stakeholders, including regional or international cooperation is required for securing cyberspace. However, many states are struggling with addressing cyber security through public private cooperation (PPC).

[16] ITU website 2010
[17] ITU website 2010

PPCs and the challenges of information sharing:

- The private sector is understandably reluctant to share sensitive proprietary information about intrusions, actual damage, theft and crime, as well as prevention practices, with either government agencies or competitors because information sharing is a risky proposition with less than clear benefits. No company wants information to surface that they have given in confidence, since such an event could jeopardize their market position, customer base or capital investments.
- Nor would private companies risk voluntarily opening themselves up to costly and time-consuming litigation. Industry fears that breaches on innocent customers might inadvertently occur during investigations. Negative publicity or exposure as a result of reports of information infrastructure violations could lead to threats to investor and consumer confidence in a company's products. Moreover, companies fear revealing trade secrets to competitors, and hence are reluctant to share proprietary information. They also fear that sharing this information with government may lead to increased regulation of the industry or of e-commerce in general.
- In addition, there might be a lack of trust towards law enforcement, or a concern that company systems may become caught up in an investigation and lose production or development time. Hence, many private sector enterprises, including banks, find it easier to keep quiet and absorb the pain inflicted by computer attacks and intrusions. Moreover, few high tech companies are interested in being perceived by their customers as active agents of law enforcement. Government agencies, meanwhile, are all too often viewed as demanding this type of information from the private sector, but giving back little in return. Thus, there are huge disincentives to report cyber intrusions.
- The prospect that confidential business information would be subject to public disclosure under other statutes if shared with government, such as the Freedom of Information Act for example, can become a barrier to information sharing that is difficult to surmount.
- On the other hand, many private sector mechanisms for information sharing already exist without the need for government intervention. For example, both the "white-hat hacker" and the security researcher community provide a valuable private sector service. They are active information sharers which head off a vast number of attacks and identify vulnerabilities before harm occurs. Particularly on the technical level, information sharing about vulnerabilities and remediation happens routinely in the private sector. This is not because of a mandate from government. Rather the impulse to share is based on a well-grounded exchange of network-protective information done by engineers of, for example, the major telecom companies. And if the government wants to join in the sharing, they would be welcome—that is, if they bring added value to the arrangement.
- There is an urgent need for active, robust, and credible liaison of government with the private sector. Government agencies have to respect the confidentiality as well as the value of the information and secrets that the private sector may give them to do their job. In order to do the job on both sides, real-time feedback on information sharing is essential. All partners engaged in ensuring IT security will not share information unless they have a high degree of confidence that this information will be protected from disclosure. Hence, all partners must take steps to protect sensitive data as a precursor to information sharing. Only then will it be possible to form trusted relationships and begin data sharing. Similar principles apply to information sharing between governments and international organisations.

Three attributes are unique to a cyber security partnership, which engender some complications: (1) issues of property in the cyber realm, both intellectual and in asset valuation, may not have direct parallels to existing concepts of property addressed in other PPC arrangements (2) traditional PPC operates under established regulatory structures built around a variety of local, regional, federal, international and mixed authorities. Such a set of authorities, or regulatory structure, does not exist in the cyber domain. In addition, companies have been, and may remain, unwelcoming to the idea of regulation on the Internet. (3) the time scale involved in cyber development, incident, response and threat indications are all vastly shorter than anything in traditional PPC.

The question of information-sharing is also of critical importance. One would think that identifying and communicating about new cyber threat developments would be relatively simple to achieve. It is not. No consensus exists on precisely what that means, or whether it would truly be effective. What information needs to be shared by the government with the private sector and what from the private sector should be shared with government? How would it make a difference? And how will the recipient use the information?

The mission of cyber security PPC, broadly defined, is to establish reasonable standards and best practices such that anomalous activities and behaviours can be identified. This identification then allows for notification, provided to users and suppliers alike, of the existence of these behaviours and vulnerabilities across processes and technology, enabling remedial action to minimize or prevent loss of assured access or privacy for users.

To be effective, the partnership needs to provide three capabilities essential to cyber security: (1) detection: the partnership must define, identify and watch for behaviour of concern; (2) protection: it must ensure compliance with the partnership's security standards, sanctioning those who fail to comply; and (3) response: which must provide a means to conduct forensic examinations following disruptions, analyze vulnerabilities, fix security shortcomings, and effectively attribute attacks to their perpetrators. However, these activities, as well as incentives for greater participation and sanction for failures in conduct, need to be agreed to and accepted by all parties: suppliers, users, and government.

Other components that may be included are: (1) inspection and enforcement of standards upon suppliers and Internet Service Providers (ISPs); (2) the ability to watch networks, search for and analyse future threats, and warn all users before an emergency occurs; (3) the ability to respond to attacks, through warnings and technical fixes, as well as to plan for the recovery of crucial systems after an emergency; (4) necessary protection of privacy and free speech, individual rights and business concerns, cognizant of government needs; and (5) mechanisms for international collaboration on cyber security.

To be effective, a model of PPC for cyber security needs to represent the interests of parties whose concerted and agreed behaviour can produce the desired outcomes. This means that the partners must be: (1) broadly recognized as having a sufficiently high stake in and motivation or incentive to improve cyberspace security; (2) be able to demonstrate that in advancing their interest they are also advancing the wider public interest; and (3) be sufficiently few in number to operate effectively—that is small enough to retain the ability to act quickly, but at the same time broadly representative, and capable of influencing the behaviours of the constituent elements of the partnership.

The constituencies to be represented should include: (1) Suppliers—a constituency that can be nearly as broad as the user set, depending on the purpose of the partnership. The makeup could range from content suppliers, internet service providers (ISPs), and software and hardware producers to telecommunications and mobile phone companies. (2) Users—ordinarily thought of as individuals, but which include small and large businesses, organisations, associations, as well as government entities. These users are both domestic and foreign. And (3) Government—that has two important and distinct roles. First, it is a regulator of the market in its role as the protector of public interests. Second, it is a massive consumer of Internet services and is heavily dependent on those services to communicate with, and provide for, its citizens.

Finally, one should keep in mind that from the private sector perspective, participation in PPC involves real costs, ranging from time committed to opportunity lost due to participation. In fact, some industry partners dedicate full time personnel just to participate in these activities. Moreover, when industry participates in PPC, it may lead to reputational or brand risk, to expenditure of unforeseen legal fees, and could cost political capital as they may be seen as partisan as a result of participation in the activity.

2.4 THE RESPONSE: INTERNATIONAL COOPERATION

As national governments continue in growing numbers to identify cyber-security as a top national security priority, the time may indeed be ripening for reaching agreement on an international set of cyber-laws. “The UK Armed Forces Minister Nick Harvey has called for governments across the world to establish laws governing cyberspace and how it is used. In a speech to international affairs think-tank Chatham House in London, he said it was only a matter of time before terrorists begin to use cyber space more systematically, not just as a tool for their own organisation, but as a method of attack, according to BBC News. The UK government has pledged to spend £650m in the next four years on a National Cyber Security Programme to protect individuals and the national infrastructure from cyber attacks.“[18]

The USA has also recently made cyber security a key priority, establishing the US Cyber Command: “Given our increasing dependency on cyberspace, this new command will bring together the resources of the department to address vulnerabilities and meet the ever-growing array of cyber threats to our military systems,” Secretary of Defense Robert M. Gates announced on the 21st of May 2010.[19]

The recent Russian cyber crime treaty proposal (although rejected by the UN and notably by Canada, the US and the EU) shows there is a growing momentum in trying to achieve commonality on cyber security issues, despite the fact that key hurdles remain in trying to reach agreement on how precisely to harmonize different standards and legal systems.

[18] ComputerWeekly.com, 10 November 2010.

[19] http://www.af.mil/news/story.asp?id=123205791

Perhaps the most solid example of an international treaty addressing cyber crime is the Council of Europe's Convention on Cyber Crime. The convention has been ratified by thirty countries, including the USA, and "aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation."[20]. It also provides for better coordination of cross-border investigations among signatories and a "26/7" alert system for cyber attacks. The EU's Stockholm program, adopted last year, envisages further measures to get a better grip on cyber crime. The European commissioner for home affairs is expected to present a new "security strategy," including a draft regulation on improving protection against attacks on networks and information systems.

Like NATO and other organisations in recent years, the EU has been increasingly active on cyber security issues including the establishment of ENISA, the European Network and Information Security Agency, which contributes in an essential manner to achieve a high level of network and IT security within the EU. Furthermore, in 2006, the EU adopted a Strategy for a Secure Information Society. The 2008 Report on the Implementation of the European Security Strategy includes cyber security as one of the global challenges and key threats.[21] In March 2010, the European Council adopted the EU's Internal Security Strategy, which describes cyber crime as a global, technical, cross-border, anonymous threat to IT systems. Later this year, the EU Commission will adopt a Communication on the Internal Security Strategy, which will include action-oriented proposals.

At the end of the day, protecting cyberspace and the digital infrastructure is a shared responsibility of governments, private sector participants, and also regional and international organisations. Although some may argue that government must take charge, achieving success here will require actions from all, including partnerships between governments, within the private sector, between governments and the private sector, and between all of these with regional and international organisations. To achieve this, a cyberspace and cyber security threat and vulnerability information clearinghouse could be created. This clearinghouse, if organised as a non-profit institution, could act as a trusted facilitator and broker of information between all stakeholders.

Even as we grapple with the complex problems identified in this paper, it is clear that these are just the tip of the iceberg. New challenges, for which we don't yet fully understand the implications, are continuously emerging.

[20] Council of Europe, Convention on Cyber crime, European Treaty Series – No. 185, Budapest, 23 November 2001 http://conventions.coe.int/Treaty/en/Reports/Html/185.htm)

[21] A Strategy for a Secure Information Society –"Dialogue, partnership and empowerment", Brussels, 31 May 3006, COM(2006)251, and: Report on the Implementation of the European Security Strategy – Providing Security in a Changing World, Brussels, 11 December 2008, S407/08.

A future cyberspace treaty:[22]

> Hamadoun Touré, Secretary-General of the UN International Telecommunications Union (ITU), has called for a comprehensive "cyber treaty" that would have a built-in legal and regulatory framework, as well as cross-continent contingency plans in the event of large-scale cyberattacks .
>
> "We need to have an international framework to make cyberspace peaceful," said Touré at a recent conference, adding that no nation is immune from potential threats. "People who think they are secure don't want anyone else to talk about it. I say there is no online superpower."
>
> The ultimate goal, according to Touré, is to establish a cyberspace treaty, which will spell out acceptable and unacceptable behaviour and put the obligation on each country to police its own cyberspace. Touré says a fundamental shift has taken place in cyberspace and that the world is currently ill-equipped to deal with it diplomatically.

How will we define what constitutes a cyber-attack and what kind of retaliation is realistic, effective and appropriate? In a situation where it is very difficult to identify your attacker, your attacker may be hiding behind a neutral middleman, and where your attacker has in many cases no assets on which to inflict serious retaliatory damage, retaliation, as it has been known to date, no longer exists. Does this mean that the military and defence departments will have to stay one step ahead of the attacker with constantly evolving and innovative software and hardware? Is this realistic? Given the time and budgetary measures required to realize software development within a government context, how can governments and/or militaries even hope to be quicker, faster and more agile than the cyber-enemy? Are states already de facto in the process of abdicating their responsibility for the security of citizens and key business sectors to private cyber-security firms? How can this trend be reversed?

In turn, what will this mean for the IT sector as a whole given its strategic importance as the most critical industry sector for a nation's economic and military competitiveness? Will it become the next defence industry?

Another set of challenges will relate to the fact that cyberspace is no longer the free, interoperable, multi-user World Wide Web it once was. There is a clear move toward a fragmentation of cyberspace for multiple reasons from national boundaries and censorship, to language and to the increasing popularity of apps designed only for specific devices leading to semi-closed or closed sub-groups of web users. The impact of this trend on cyber-security policy is as yet unknown or un-examined. Are we moving into an age of internet protectionism? What will this mean?

Finally, what about privacy and identity in an age of heightened cyber-security? Cyber-defence is widely recognized by defence departments and the military as the next theatre of war and a key priority for national security. How will this increased focus on cyber-security affect the web as we know it today? Will cyber-security take precedence over freedom? New software designed to track, analyse and aggregate information from social networking sites is increasingly being used for counter-

[22] Tim Gray, TechNewsDaily, 9/10/2010

terrorism purposes, to monitor conflict situations and criminal networks, and to police at the local, national and international level. There is a growing acceptance of its effectiveness, in particular in its ability to map behaviour, predict criminal activity and identify key terrorist or criminal actors. This is all positive, but have we given enough thought to the peripheral uses of new technology designed primarily for defence purposes? What about its potential use for employers, marketing agencies and others to monitor individuals' behaviour at work and online? Will privacy exist in the future?

Key entities and efforts that address global cyberspace security and governance:[23]

There are some twenty key entities and efforts whose international activities significantly influence the security and governance of cyberspace. Although they do not represent all international cyber-related entities and efforts, they are consistently identified as key players. These range from information-sharing forums that are non-decision-making gatherings of experts to private organisations to treaty-based decision-making bodies founded by countries. Their efforts include those to address topics such as incident response, technical standards, and international or regional law enforcement cooperation. These entities have ongoing initiatives that involve governments and private industry stakeholders to address a broad set of topics, such as the implementation of incident response mechanisms, development of technical standards, the facilitation of criminal investigations, and the creation of international policies related to IT security and critical infrastructure protection.

These key entities are:

- Asia-Pacific Economic Cooperation
- Association of Southeast Asian Nations
- Council of Europe
- European Union
- Europol
- Forum of Incident Response and Security Teams
- Group of Eight
- Institute of Electrical and Electronic Engineers
- International Electrotechnical Commission
- International Organisation for Standardization
- International Telecommunication Union
- Internet Corporation for Assigned Names and Numbers
- Internet Engineering Task Force
- Internet Governance Forum
- Interpol
- Meridian
- NATO
- Organisation of American States
- Organisation for Economic Cooperation and Development
- United Nations

[23] See Annex 1 for what they do.

3. Conclusions

Building on the issues discussed in this paper, outlined below are some key measures, which could be taken to improve individual, corporate, national, regional and international cyber-security:

Proposed measures needed for discovering and monitoring cyber threats and risks are:

- Establishing real-time surveillance, monitoring, and early-warning capability of attacks, and a capability for sharing critical incident response information with key stakeholders.
- Implementing intrusion detection systems using passive sensors to identify when unauthorized users attempt to gain access to networks and IT systems.
- Strategically addressing identity management, authentication, credential and access management to provide greater assurance that only authorized individuals and entities can gain access to IT systems across government and critical infrastructure.
- Developing malicious code detection methods that go beyond simple signature detection, for long-term proactive detection and analysis, which can identify mutations of variations of malicious code with high accuracy and low false positive rates.
- Developing methods for determining the source of malicious code or behaviour through analysis of network topology and/or traffic that also work in the presence of IP spoofing, a large number of compromised machines, mutating malware, and so forth.
- Developing online learning methods for dynamic modelling, for modelling data with skewed class distributions, and feature selection for data with evolving characteristics.
- Establishing deep-packet inspection scanners at every Tier 1 Internet Service Provider (ISP) that connect directly to most other ISPs, in order to stop malware entering a backbone before it reaches the network it was intended to attack.

Proposed measures needed for countering cyber threats and risks are:

- Achieving a more reliable, resilient and trustworthy digital infrastructure for the future.
- Developing comprehensive and robust means and methods that ensure quick and irrefutable attribution of attacks.
- Developing a Cyber Security Strategy, designed to shape the international environment, and to bring like-minded nations together on issues such as

technical standards, acceptable norms, sovereign responsibility, and the use of force.

- Carrying out comprehensive assessments of the vulnerabilities of key resources and critical national infrastructures, including risk assessments to determine risks posed by particular types of attacks.
- Developing a comprehensive national plan to deal with these vulnerabilities.
- Establishing priorities for protection, while acknowledging that not all assets are equally critical, and that the costs associated with protecting assets must be balanced against the benefits of increased security according to the threat.
- Integrating all relevant information, analyses, and vulnerability assessments in order to identify priorities for protective and support measures, identifying potential risk mitigation activities, and for prioritizing these based on cost-effectiveness.
- Better defining roles, lead-responsibility and accountability of government entities in securing critical national infrastructures, government networks, and IT systems.
- Safeguarding networks and IT systems by reducing potential and actual vulnerabilities, protecting and defending against intrusion attempts, anticipating future threats, shaping the future environment by enhancing research and development, education, and by investment in leap-ahead technologies.
- Correcting weaknesses in risk assessments, IT security policies and procedures, security planning, security training, system tests and evaluations, remedial actions that need to be taken, and guiding principles.
- Correcting IT security deficiencies related to user identification and authentication, authorization, boundary protection, audit and monitoring, cryptography, physical security, segregation of duties, configuration management, and contingency planning.
- Protecting against disruption of operations of IT systems for critical infrastructure and ensuring that any disruptions that occur are infrequent, of minimal duration, manageable, and cause the least damage possible.
- Making concerted and collaborative research and development in cyber and critical infrastructure security a national priority, while ensuring that it contains short-term, mid-term and long-term cyber security priorities, includes input from the private sector and academia, and is consistent with the Cyber Security Strategy.
- Establishing working groups charged with conducting annual reviews of research and development initiatives in their sectors, and recommending

updates to the priorities based on changes in technology, threats, vulnerabilities, and risk.

- Encouraging the private sector to perform periodic vulnerability assessments of critical IT and telecommunication systems in their parts of CNI.
- Establishing metrics and measures to determine the effectiveness of projects in making networks and IT systems more secure, and to track progress against those measures that can create powerful incentives to influence organisational and individual behaviour, and timely submission of development deliverables.
- Conducting performance audits in accordance with generally accepted government auditing standards.
- Establishing effective coordination and information sharing between public and private sector participants in response to significant cyber incidents.

Proposed measures needed to solve the legal challenges are:

- Establishing, reviewing, and modernizing criminal law, procedures for electronic investigations, and policy to ensure the capability exist to prevent, deter, respond to, and prosecute cyber crime, both on the domestic and international levels.
- Creating acceptable legal norms for dealing with cyber crimes regarding territorial jurisdiction, sovereign responsibility, and use of force.
- Establishing dedicated cyber crime units, electronic forensics, training, and outreach for all who have a role in organising a unified response to cyber incidents and deterring cyber crime, including the judiciary and the private sector.
- Establishing, reviewing, and updating legal infrastructures related to data protection, privacy, digital signature, commercial law, e-government, and encryption in close consultation with privacy experts across government and of civil society.
- Reconciling differing national laws concerning investigation and prosecution of cyber crimes, data protection, preservation, and privacy, and addressing the problem of existing cyber laws of other countries that do not carry enforcement provisions.
- Developing interagency mechanisms to coordinate engagement and ensure information sharing with international partners on cyber incident investigations.
- Establishing a well-coordinated whole-of-government approach in conducting international outreach and interactions with international entities to address cyber security strategically, which includes facilitating cooperation between cyber security and law enforcement professionals in different nations,

developing security standards, and pursuing international agreements on engagement and secure information sharing.

- Establishment of a process for proposing and refining rules of engagement, negotiating related agreements with foreign governments, and for coordinating responses to international cyber incidents.
- Assisting in developing international norms and standards, and enabling and facilitating international and regional cooperation.
- Streamlining and clarifying elements of the legal structure to support assurance measures, including clearing jurisdictional barriers to attribution of attacks and pursuing hackers electronically.

Proposed measures needed to create a skilled cyber workforce and public awareness to promote cyber security are:

- Overcoming the major challenges in attracting, hiring, training, retaining, and effectively managing cyber security and forensics talent, and introducing more attractive career tracks.
- Reaching agreement among all stakeholders on the scope of educational efforts and projects to ensure that an adequate cadre of skilled personnel is developed to protect IT systems, prioritizing and redirecting educational efforts to build a professional cyber workforce, and ensuring the development of skilled individuals for future government employment.
- Initiating a national public awareness and education campaign to promote cyber security, to expand support for key education programs, and research and development to ensure the nation’s continued ability to compete in the information age economy.

The keys for creating an effective Cyber Security Strategy are:

- Develop a Cyber Security Strategy that clearly articulates strategic objectives, goals, and priorities.
- Establish top-level government responsibility and accountability for leading and overseeing the national cyber security policy.
- Establish a governance structure for the strategic implementation of the Cyber Security Strategy.
- Publicize and raise awareness about the seriousness of the cyber security problem.
- Create an accountable, operational cyber security organisation leading the implementation.

- Focus action more on prioritizing assets, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.
- Bolster public private partnerships through an improved value proposition and use of more incentives.
- Focus much greater attention on addressing the global aspects of cyberspace.
- Improve law enforcement efforts to address malicious activities in cyberspace.
- Place greater emphasis on cyber security research and development, including consideration of how to better coordinate government and private sector efforts.
- Increase the cadre of cyber security and forensics professionals.
- Make the government a model for cyber and CNI security, including using its acquisition function to enhance cyber security aspects of products and services.

Annex:

Key entities and efforts with significant influence on international cyberspace security and governance

Asia-Pacific Economic Cooperation (APEC)

APEC is cooperative economic and trade forum designed to promote economic growth and cooperation among 21 countries from the Asia-Pacific region. APEC's Telecommunication and Information Working Group (TEL) is to support security efforts associated with the information infrastructure of member countries through activities designed to strengthen effective incident response capabilities, develop information security guidelines, combat cyber crime, monitor security implications of emerging technologies, and foster international cooperation on cyber security. The working group has pursued some of these activities with other international organisations, such as ASEAN, ITU, and the OECD.

Association of Southeast Asian Nations (ASEAN)

ASEAN is an economic and security cooperative comprised of 10 Southeast Asian nations. According to the 2009-2015 Roadmap for an ASEAN Community, it seeks to combat transnational cyber crime by fostering cooperation among member-nations' law enforcement agencies and promoting the adoption of cyber crime legislation. In addition, the road map calls for activities to develop information infrastructure and expand computer emergence response teams (CERT) and associated drills to all ASEAN partners.

Council of Europe

The Council of Europe is an organisation of 47 member countries founded in 1949 to develop common democratic principles for the protection of individuals. In 2001, it adopted a Convention on Cyber crime to improve international cooperation in combating actions directed against the confidentiality, integrity, and availability of computer systems, networks, and data. The convention identified agreed-upon cyber-related activities that should be deemed criminal acts in countries' domestic law. These acts included illegal access to computer systems, computer-related fraud, activities involving child pornography, and copyright infringement. The Council of Europe also sponsors training and conferences to address cyber security issues.

European Police Office (Europol)

Europol, the European Police Office set up in 1992, is a specialized institution of the EU whose task and purpose is to facilitate international police cooperation in the fight against organised crime, terrorism, and cyber crime. Europol's mission is to make a significant contribution in the areas of uncovering, preventing and prosecuting organised crime and combating the actions of organised criminal organisations. It supports member states by facilitating the exchange of intelligence between Europol and Europol Liaison Officers, seconded to its headquarters in The Hague by the member states as representatives of their national law enforcement agencies. In June 2010, an EU Cyber crime Task Force was established that includes the Internet Crime Reporting Online System (ICROS), the Analysis Work File Cyborg that is actively working to fight criminal groups operating on the Internet, and the Internet & Forensic Expert Forum (IFOREX) to host technical data and training for cyber crime law enforcement. The Europol Strategy 2010-2014 includes a clear plan for the strengthening of cyber crime capabilities which will include the creation of the European Cyber crime Center at Europol that will coordinate and ensure an effective action to fight cyber crime at European level. It will acquire new data processing tools and create databases on high-risk Internet sites. Europol is providing operational analysis, expertise and technical support for investigations and operations within the EU, and is generating strategic reports and crime analysis on the basis of information and intelligence supplied by national law enforcement agencies like police, customs, immigration services, or gathered from other sources. In order to fight international organised crime effectively, Europol cooperates with a number of third countries and institutions such as the European Central Bank, the European Monitoring Center for Drugs and Drug Addiction, the European Anti-Fraud Office OLAF, the UN Office on Drugs and Crime, the EU Joint Situation Center, the World Customs Organisation, and many more.

European Union (EU)

The EU is an economic and political partnership among 27 European countries. Subcomponents of its executive body—the European Commission—are to engage in cyber security activities designed to improve (1) preparedness and prevention, (2) detection and response, (3) mitigation and recovery, (4) international cooperation, and (5) criteria for European critical infrastructure in the information communication technology sector. The European Commission will prioritize international engagement involving mutual assistance, recovery efforts, and crisis management. It also formed the European Network and Information Security Agency (ENISA), an independent European agency created to enhance the capability of its members to address and respond to network and IT security problems. Established in 2004, ENISA's international outreach is to primarily focus on information infrastructure protection and resilience, awareness raising, and the exchange of information among its members. Moreover, there are several independent organisations within the EU that develop technical standards. The European Committee for Standardization is to work to remove trade barriers for European industry and provide a platform for the development of European standards and technical specifications. The European Committee for Electrotechnical Standardization is a non-profit technical organisation responsible for preparing voluntary electrotechnical standards for electrical and electronic goods and services in the European market. The European Telecommunications Standards Institute is a non-profit organisation responsible for producing globally applicable standards for information and communications techno-logies, including those supporting the Internet.

Forum of Incident Response and Security Teams (FIRST)

FIRST is an international confederation of individual CERTs that work together to share technical and security incident information. It includes over 220 members from 42 countries. The members' incident response teams represent government, law enforcement, academia, the private sector, and other organisations. FIRST's steering committee is responsible for its general operating policy, procedures, and other matters affecting the organisation. FIRST has worked with multiple international standards organisations to develop standards for caber security, incident management and response. In addition, it uses the Common Vulnerability Scoring System as a standard method for rating IT vulnerabilities, which helps when communicating vulnerabilities and their properties to others.

Group of Eight (G8)

G8 is an international forum that includes the governments of Canada, France, Germany, Italy, Japan, Russia, the UK and the US. The G9's cyber security efforts are directed by the G8 Subgroup on High-Tech Crime, which seeks to prevent, investigate, and prosecute crimes involving computers, networked communications, and other new technologies. In 1997, the subgroup created the 24-7 High-Tech Crime Point-of-Contact Network, which allows law enforcement officials from countries—including those from outside the G8—to quickly contact their counterparts in other participating nations for assistance with cyber crime investigations. The network supplements traditional methods of obtaining law enforcement assistance. In 2004, the subgroup also developed a best practices guide for network security to assist network operators and system administrators when responding to computer incidents. And in 2006, during its chairmanship of the G8, Russia advanced an initiative for public private partnerships to counter terrorism and organised crime, and cyber security was one of the three priority areas, alongside critical energy infrastructure protection and cross-border movement of people, goods, and money, which also included cyber security aspects.

Institute of Electrical and Electronic Engineers (IEEE)

The institute is a professional association focused on electrical and computer sciences, engineering, and related disciplines. Its cyber security-related activities include the development of technical standards through the IEEE Standards Association, which follows consensus-based standards development processes. Among other things, standards include an internationally recognized standard that addresses encryption and wireless networking. In addition, the IEEE Standards Association has been involved with the US National Institute of Standards and Technology to draft cyber security standards for electric utility control systems.

International Electrotechnical Commission (IEC)

The IEC prepares and publishes international standards for electrical, electronic, and related technologies. Its membership includes national committees from over 70 nations, which are comprised of representatives from each country's public and private sector. The IEC and the International Organisation for Standardization (ISO), through a joint technical committee (JTC), have developed information security standards for all types of organisations, including commercial enterprises, government agencies, and non-profit organisations. For example, one of this jointly developed standard addresses the development and maintenance of information security management systems and security controls that protect information assets, which is applicable to all organisations regardless of size.

International Organisation for Standardization (ISO)

ISO is a NGO that develops and publishes international standards through a consensus-based process involving a network of the national standards institutes of 162 countries with a Central Secretariat in Geneva supporting the process. Its standards include those for traditional activities such as agriculture and construction, as well as those for the latest in information and communication technology.

The International Telecommunication Union (ITU)

ITU is a UN agency whose mission includes developing technical standards, allocating the radio spectrum, and providing technical assistance and capacity-building to developing countries. Three sectors carry out these missions by promoting recommendations: the ITU-telecommunication Standardization Sector (ITU-T), the ITU-Radiocommunication Sector (ITU-R), and the ITU-Telecommunication Development Sector (ITU-D). In addition, the ITU General Secretariat provides top-level leadership to ensure that institutional strategies are harmonized across all sectors. ITU members include delegations from 191 nations, as well as more than 700 members from the private sector. ITU has developed technical standards for security and is engaged in other cyber security activities. For example, IZU-T has established a study group for telecommunications security to focus on developing standards and recommendations associated with network and information security, application security, and identity management. ITU-D, through its members' efforts, prepared a report on cyber security best practices for countries seeking to organise national cyber security efforts. And the ITU General Secretariat issued a Global Cybersecurity Agenda (GCA) designed to promote a comprehensive and coordinated international approach to cyber security across all ITU sectors. The GCA covers five areas: (1) legal measures, (2) technical and procedural measures, (3) organisational structures, (4) capacity building, and (5) international cooperation. Moreover, the General Secretariat signed a memorandum of understanding with the International Multilateral Partnership Against Cyber Threats that will establish an operations center to coordinate incident response and to provide cyber threat information to member countries and the private sector.

Internet Corporation for Assigned Names and Numbers (ICANN)

ICANN is a private US non-profit corporation whose primary function is the coordination of the technical management of the Internet's domain name and addressing system. It is overseen by a board of directors composed of 21 representatives, including 15 voting members and 6 nonvoting liaisons. ICANN signed an Affirmation of Commitments with the US Department of Commerce in 2009, which completed the transition of the technical management of the DNS to a private-sector led multistakeholder model that is intended ensure accountability and transparency in its decision-making with the goal of protecting the interests of global Internet users. ICANN is facilitating DNS policy development through a bottom-up process involving diverse interests of generic and cou8ntry code top-level domain registries, domain name registrars, the regional Internet registries, the technical community, business and individual Internet users, and governments. It also performs the Internet Assigned Names Authority function under contract to the US Department of Commerce. This Authority's functions consist of several independent Internet management responsibilities, including coordination of the assignment of technical protocol parameters, performance of administrative functions associated with root zone management, and the allocation of Internet numbering resources.

Internet Engineering Task Force (IETF)

IETF is a technical standards-setting body responsible for developing and maintaining the Internet's core standards, including the DNS protocol and its security extensions and the current and next-generation versions of the Internet Protocol. The core standards the IETF develops define, on a basic level, how the Internet operates and what functions it is capable of performing. It is a voluntary, consensus-based standards body, whose participants include network operators, academics, and representatives of government and industry, among others. Much of IETF's work is conducted via e-mail lists, although it does host three meetings at locations around the world each year.

The Internet Governance Forum (IGF)

The 2005 World Summit on Information Society's Tunis Agenda mandated that the UN Secretary General create the IGF as a multistakeholder venue to discuss public policy issues related to key elements of Internet governance. The IGF's broad membership and emphasis on information exchange enable it to serve as a uniquely important forum for foreign governments, the private sector, civil society organisations, and individuals to engage in open discussion without being preoccupied with advocating a particular policy outcome. Although the annual meetings do not directly result in standards, recommendations, or binding agreements, ideas generated by the IGF can contribute to outcome-oriented efforts at other international organisations.

INTERPOL

INTERPOL is the world's largest international police organisation created to facilitate cross-border police cooperation. It collects, stores, analyzes, and shares information related to cyber crime between its 188 member countries through its global police communications system. It is also responsible for coordinating operational resources such as computer forensic analysis in support of cyber crime investigations. It has a network of investigators in national computer crime units to help law enforcement seize digital evidence as quickly as possible and facilitate cooperation when a cyber attack involves multiple jurisdictions. To develop strategies for emerging cyber crime methods, it assembles groups of experts into regional working groups that harness the regional expertise available in Europe, Asia, the Americas, the Middle East, and North Africa. The working party activities are to include sharing information ob regional cyber crime trends, enhancing cooperation among member countries, and developing educational materials for law enforcement.

Meridian

Founded in 2005, the Meridian Conference and Process aims to exchange ideas and initiate actions for government-to-government cooperation on critical information infrastructure protection issues globally. An annual conference and interim activities are held each year to help build trust and establish relationships within the membership to facilitate sharing of experiences and good practices on critical information infrastructure protection from around the world. Participation in the Meridian Process is open to all countries and aimed at senior government policymakers. The conference allows participants to explore the benefits of and opportunities for cooperation between governments and share best practices. The Meridian Process also seeks to advance collaborative efforts on specific topics such as control systems security.

North Atlantic Treaty Organisation (NATO)

NATO is an alliance of 28 countries from North America and Europe. It approved a Cyber Defense Policy in 2008 to provide direction to its member nations to protect key information systems and support efforts to counter cyber attacks. Specifically, the policy established the Cyber Defense Management Authority, which has authority for managing cyber defense crises, to include directing the NATO Computer Incident Response Capability. After the Estonian government, law enforcement, banking, media and Internet infrastructure endured three weeks of cyber attacks in April, NATO also encourages the creation of state-sponsored cyber defense authorities to exchange information, define the scope of mutual support in the event of an identified cyber incident, and to identify communication and information systems that handle information deemed critical to the alliance.

Organisation of American States (OAS)

OAS is an intergovernmental organisation comprised of 34 nations in North, Central, and South America, as well as island nations in the Caribbean. In 2004, OAS member states adopted the Inter-American Comprehensive Strategy for Cybersecurity,which identifies cyber security as an emerging threat to OAS member states and requires 3 OAS entities to take action to address different aspects of cyber security. Specifically, the strategy directs the Inter-American Committee against Terrorism (CICTE) to develop plans for the creation of a hemisphere-wide 24-hours, 7 days-per week network of Computer Security Incident Response Teams. In addition, the strategy directs the Inter-American Telecommunication Commission (CITEL) to evaluate existing technical cyber security standards, recommend the adoption of particularly important cyber security standards, and identify obstacles to implementing those standards within the Americas. Finally, the strategy directs the Meetings of Ministers of Justice or Other Ministers or Attorneys General of the Americas, through the Group of Government Experts on Cyber-Crime, to provide technical assistance to member states in drafting and enacting effective computer crime laws to protect information systems and facilitate investigations and prosecutions.

Organisation for Economic Cooperation and Development (OECD)

OECD is an intergovernmental organisation composed of 31 democratic countries. Member countries' governments can compare policy experiences, seek answers to common problems, identify best practices, and coordinate domestic and international policies. The OECD Working Party on Information Security and Privacy (WPISP) uses a consensus-based process to develop policy options to address the security and privacy implications of the growing use of information and communication technologies. In addition to developing policy analysis, OECD is responsible for making recommendations designed to improve the security and privacy of its member countries. For example, in 2008, the OECD Council adopted a recommendation calling for member countries to cooperate among themselves and with the private sector to improve the protection of critical information infrastructure. Specifically, the recommendations called for bilateral and multilateral sharing of best practices, development of common understandings of cross-border interdependencies and vulnerabilities, identification of national agencies involved in critical information infrastructure protection, acknowledgment of the value of international watch and warning networks, and international cooperation on cyber research and development.

United Nations (UN)

The UN is an international organisation with 192 member countries founded in 1945 and chartered to maintain international peace and security, develop friendly relations among countries, and promote social progress, better living standards, and human rights. The General Assembly, which provides a forum for discussing and adopting resolutions on cyberspace-related issues and raising international cyber security awareness, is the UN's chief deliberative, policymaking, and representative body. In 2005, the UN Interregional Crime & Justice Research Institute began to address cyber crime-related issues, which is building the Hackers Profiling Project (HPP). Other organisational entities within the UN, such as the Office on Drugs and Crime, are additional forums where member countries can discuss approaches for transnational issues, including cyber crime.

About the series

DCAF's Horizon 2015 project explores the role of a wide range of private and other non-state actors in responding to the newest security governance challenges. This project aims to broaden our analytical horizons 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-issue" approach.

DCAF's Horizon 2015 project brings together relevant state and non-state actors for a series of thematic roundtables throughout 2010 and 2011. 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* available at www.dcaf.ch/Publications – that seeks to describe the current security landscape and provide a background to the project's work as a whole.

Other titles in the series:

Democratic Challenges of Cyber Security, Benjamin S. Buckland, Fred Schreier, Theodor H. Winkler

Public Private Cooperation: Challenges and Opportunities in Security Governance, Benjamin S. Buckland,Theodor H. Winkler

Private Military & Security Companies: Future Challenges in Security Governance, Anne-Marie Buzatu, Benjamin S. Buckland

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