TED ROGERS SCHOOL OF MANAGEMENT RYERSON UNIVERSITY

PRIVACY AND CYBER CRIME INSTITUTE

Securing Cyberspace:
A Comparative Review of Strategies Worldwide

by
Avner Levin (Director)
Paul Goodrick & Daria Ilkina (Research Associates)

Table of Contents

Executive Summary
Several distinct cyber-blocs have formed with their unique cyber-security strategies and emphases. The Anglosphere, led by the US and the UK, emphasizes a leading private sector role, an educated workforce, and outreach and diplomacy. The EU, led by Germany, focuses on a robust legal and regulatory framework, and on the promotion of the Council of Europe (Budapest) Convention of Cybercrime as a blueprint for international cooperation and enforcement. The Baltic States are in tight cooperation with NATO in the development of their national cyber-security strategies. The post-Soviet CIS bloc, led by Russia with some degree of Chinese cooperation, focuses on internal threats, abhors extra-territorial judicial action, and promotes a corresponding international framework under the auspices of the UN.

Most cyber-strategies, with the notable exceptions of Russia, China and their allies, are compatible with Canadian interests. Strategies generally differ on the roles that they allocate to the public and private sectors, and within those, on the roles allocated to policy, regulation, for-profit and not-for profit ventures as promoters of cyber-security. Strategies also direct a wide range of resources in a variety of ways. The majority of countries reviewed are in the process of developing and implementing their cyber-security strategies, and setting the focus of their efforts. These rapidly occurring changes in strategies and policy implementation add to the challenge of determining best practices for securing cyberspace while protecting civil liberties.

Information on the origin and ultimate target of many cyber-threats is contradictory due to the difficulty of pinpointing sources and destinations with ultimate certainty solely by technological means. China, for example, the current "cyber-villain" may be suffering from cybercrime more than commonly acknowledged and open to collaboration. Leading Western countries, such as the US and Germany, may not only be the target of attacks but the ultimate source of cyber-criminal activity as well. In order for Canada to proceed with its strategy in an informed manner, accurate, verifiable cybercrime data must be collected and evaluated to determine the optimal countries for collaboration.

As it develops its own cyber-strategy, Canada should look to global leaders and learn from the approaches of the US, UK and Germany, that emphasize education, diplomatic outreach, private sector involvement and a legal and regulatory framework that balances cyber-security and privacy.

Introduction

The pervasive feature of cyberspace is its disrespect of traditional rules and boundaries. The metaphor of an amorphous, vague, anarchic "world", "space" or "cloud" that exists outside of regular life is powerful and has gripped both public and policy. Reality may differ, but the computers and networks that connect them in the real world support the popular perception of cyberspace. Near-instantaneous communication, operation by proxy, automation of interaction and other features serve to eliminate borders and facilitate both commerce and crime. Governments face the difficult task of minimizing the latter while maximizing the former within the larger context and constraint of international relations.

This report offers a comparison of the approaches taken around the world in pursuit of these twin goals. The report first discusses the challenges that cyber-security strategies face in general, due to the features of cyberspace and international relations. It then classifies the various models and frameworks developed by various countries in order to improve cyber-security by characteristics such as the roles of the public and private sectors and the degree of cooperation with other jurisdictions. The report concludes with some recommendations as to which approaches offer the best fit with Canadian priorities and interests.

Challenges

Securing cyberspace is a Herculean and complicated task. The creation of a technological, commercial and social environment in which commerce and civic transactions are promoted and encouraged, while criminal and terrorist activities are discouraged and prevented faces numerous challenges and obstacles. The barriers to effective cyber-security are rooted both in the technological composition of cyberspace and in the political, cultural, societal and legal differences that hinder international cooperation in general. This section of the report discusses these challenges, as reported and discussed by the surveyed jurisdictions.

The International Nature of Cyberspace

The international nature of cyberspace is, in and of itself, a challenge to effective cyber-security. Since cyberspace is, in essence, a nexus of networks of computers that are physically located in many different countries and legal jurisdictions, no one country can dictate or control interactions in cyberspace.

Countries therefore attempt to enter into international agreements, either bi-lateral or multi-lateral, in an effort to regulate cyberspace and coordinate cyber-security, but these attempts are often guided by other interests and affiliations, which do not always correspond with the most effective responses to cybercrime. For example, member states of the Council of Europe have entered into a convention that does not include countries from which criminal cyber-activity is said to originate,[1] and members of the Anglosphere (the group of countries in which English is

[1] For such criticism see Alana Maurushat, *Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools?* 33 U OF NSW L. J. 431 (2010) at http://www.austlii.edu.au/au/journals/UNSWLRS/2011/20.html

the official or the most common language, such as the UK, Canada and Australia) are developing a coordinated strategy to cyber-security even though criminals in these countries may not specifically target others in the Anglosphere. Where agreement does exist between states for international cooperation, the venue for cooperation itself can be contested.

The Municipal Nature of Law

Just as cyberspace crosses borders, law, traditionally, does not. Law is inherently a municipal system, a system that regulates internal rather than external activities. In order for law to govern and regulate behaviour, it requires the ability to enforce its norms. The power to punish and sanction is always at the foundation of an effective legal system. Of course, one of the salient features of international law is its lack of enforcement powers and its foundation in voluntary cooperation amongst sovereign nations.

Attempts to coordinate legal enforcement across jurisdictions are difficult. First, jurisdictions are sovereign. Therefore, one jurisdiction has to recognize that the claims of another jurisdiction are legitimate and worthy of support. Second, rules of procedure and substance have to be agreed upon. These agreements are easier to reach between countries that share similar legal systems, such as the English Common Law system, or the European Civil Law system, but more difficult to reach between countries that do not share such similarities. Third (assuming a favourable legal outcome has been achieved), practical enforcement cooperation must be secured. It is often difficult to coordinate the practical execution of a legal decision – the arrest of a criminal, the collection of a fine – and independent agreements between law enforcement agencies and other governmental bodies must be reached.

As discussed below, to compensate for these traditional features of law and international law, countries are experimenting with a variety of approaches, such as "soft" law and voluntary codes – in which non-governmental agencies and the private, for-profit, sector play a greater role. Such approaches have been attempted in areas such as environmental protection and personal information protection, but it remains to be seen whether they will be successful when addressed at criminal individuals and organizations that have no interest or benefit in compliance.

Crime

Cybercrime and cyber-terrorism are forms of criminal and unlawful activity and, as such, pose at a minimum the same challenges to law enforcement that regular criminal activity does. Cybercrime must compete for the limited attention and limited resources of law enforcement agencies. The characterization that much of criminal online activity is "victimless" (since the majority of it is not physical), the tendency by governments and businesses to underreport cyber-intrusions, and the compensation offered by financial institutions to victims of cyber-fraud and identity theft for the bulk of their loss, have not helped cyber-security initiatives. Neither has the characterization of cybercrime as "amateurish", e.g., the product of teen hackers working out of their parents' basement, helped cyber-security initiatives become a priority.

The growing realization that criminal activity online is increasingly organized and tolerated, if not supported, by certain countries, has, however, made battling cybercrime more of a priority for law enforcement and national security agencies. The amount of attempted criminal activity (due to technology's facilitative aspects) online – the spamming, phishing and scamming that protective software deflect, dwarfs the statistics of real-world crime and is another reason for law enforcement agencies to make investigating and prosecuting cybercrime an increasing priority.

The challenge of combatting cybercrime in the context of a wider cyber-security strategy is that law enforcement is limited in reach. Some tools that may be quite effective in battling local cybercrime, for instance, the ability to cooperate with internet service providers, or to conduct surveillance, may not be as effective outside of an agency's jurisdiction. Agencies are limited in resources and they then have to rely on cooperation with other agencies, with different priorities and mandates.

Technology

Needless to say, the main reason cybercrime poses a challenge is the technology, or the technological features, that enable it. Networked computers allow for data to travel between computers at rapid speeds, and extend the reach of criminals beyond their traditional limitations. Regular crimes, such as fraud, are amplified and multiplied. The internet, in this respect, is the next enabling communication tool, following the telephone and print media before it, all of which allow for physically delimited crime to outgrow its "natural" boundaries. As is well known, the specific design of the internet as a decentralized network prevents effective control and allows criminal activity to flourish, because data paths are hard to track.

The anonymity and pseudonymity that enable free speech on the internet and are a valuable asset against tyrannical regimes allow criminal activity to flourish as well. The ability to shield an identity and physical location by technological means, through proxy servers and data routers, prevents the straightforward identification of criminals. Law enforcement and security agencies must rely on the cooperation and support of legal systems in other jurisdictions, to the extent that they can trace criminal activity to those locations. However, even when criminal activity can be traced, the distributed nature of certain cybercrimes can further complicate exact location, for legal purposes, where the crimes occurred. The cooperation of other legal systems, even in high-profile international cases, cannot be guaranteed.

Technology not only minimizes distances and increases the speed at which crimes can be committed, but also amplifies the reach of criminal activity by automating crime. The criminal is no longer physically involved, but can now send into cyberspace automated criminal agents – malware of many types. Moreover, the criminal can utilize many computers simultaneously – bot-nets – to further increase the reach of crime. The multitude of targets adds to the difficulty of demonstrating the effectiveness of particular cyber-security strategies.

Online criminal marketplaces are emerging that allow for the creation of customized malware without any programming knowledge and with minimal computer knowledge. At the other end of the spectrum, highly specialized malware can be used in increasingly sophisticated attacks to target industrial infrastructure, as with the infamous Stuxnet worm.[2] Evolving internet technology, such as the growth of mobile and "cloud" computing, offers new arenas and vectors for cybercrimes. In addition, data is regularly encrypted before transmission over the public internet and can present technical challenges even when lawful intercept has been authorized. These rapid changes in technology can result in cyber-security strategies becoming outdated before they are even fully implemented. The current limited number of individuals with the technical skills required to successfully conduct forensic investigations of cybercrimes puts law enforcement officials at a further technological disadvantage.

The Human Factor

The advantages that technology offers cybercrime are compounded by the weaknesses of human nature. Approaches to cyber-security rely on some degree of understanding, awareness and cooperation on behalf of the potential victims of cybercrime – the population at large. In fact, it is estimated that 80% or more of currently successful attacks exploit weaknesses that can be minimized through basic cyber-security practices, such as updating malware protection and software regularly.

However, it is difficult to create widespread awareness, let alone change habits and practices of computer use and online behaviour. Individuals do not feel specifically threatened as they would fearing a physical crime in the real world, and do not readily modify their behaviour as a result.

Summary

The general challenges described above highlight that cyber-security approaches must include a cooperative, international element if they are at all to be effective. Self-contained, unilateral approaches are ensured that, while they might be quite effective combating local threats to cyberspace, their success will be limited.

[2] Symantec Security Response, "Updated W32.Stuxnet Dossier is Available," Symantec Corporate, http://www.symantec.com/connect/blogs/updated-w32stuxnet-dossier-available (accessed 4 January 2012).

Approaches

This section of the report discusses the major approaches to cyber-security. An overview of each approach is provided, and the roles of the public and private sectors within each approach are discussed. As highlighted in the previous section, emphasis is placed on the degree of importance that each approach places on cooperation with other jurisdictions.

The Anglosphere

The Anglosphere is the term used to describe the group of countries in which English is the native language of the majority. The United Kingdom, Australia, New Zealand, the United States and, of course, Canada are all considered part of the Anglosphere. The Anglosphere shares more than a common language, it shares a common culture, common legal system and common values. All these make cooperation between members of the Anglosphere comparatively easy and attractive. Indeed, the five countries, also known as the Quintet, formed a Strategic Alliance Cyber Crime Working Group as early as 2006.[3] In 2011, discussions began on the harmonization of the cybercrime-related legal platform between all five countries.[4] Further in this report are the details on the approach of each country in the Quintet to cyber-security.

New Zealand

Overview

New Zealand released an updated cyber-security strategy in 2011, detailing attempts to address 3 priority areas: increasing awareness, protecting government systems, and coordinated incident response.[5]

Role of the Public Sector – Policy

According to the New Zealand approach, government is to assume a leading role in cyber-security. The Ministry of Economic Development is responsible for coordinating cyber-security policy and implementing the strategy. Several other governmental bodies play a role within the strategy:

- The National Cyber Security Centre – will provide enhanced protection of government systems and critical infrastructure as well as threat information.
- Electronic Crime Labs – will conduct forensic investigations and be accredited internationally.

[3] Federal Bureau of Investigation, "Strategic Alliance Cyber Crime Working Group," Federal Bureau of Investigation, http://www.fbi.gov/news/stories/2008/march/cybergroup_031708 (accessed 27 November 2011).
[4] Dylan Welch, "Five nations to discuss pact on cybercrime law," *Sidney Morning Herald*, 8 July 2011, Technology section at http://www.smh.com.au/technology/technology-news/five-nations-to-discuss-pact-on-cybercrime-law-20110707-1h4wm.html.
[5] Ministry of Economic Development, *New Zealand's Cyber Security Strategy*, June 2011, New Zealand Government at http://www.med.govt.nz/sectors-industries/technology-communication/pdf-docs-library/nz-cyber-security-strategy-june-2011.pdf.

- The National Cyber Crime Centre – will coordinate police response, proactively target and electronically patrol places where crime occurs, focusing on high priority areas such as organized crime, violence, and online child exploitation.
- A Computer Emergency Response Team is under consideration.

Role of the Public Sector – Law

New Zealand defined four distinct computer crimes in 2003 when it passed the Crimes Amendment Act: 1) Accessing a computer system for a dishonest purpose; 2) Damaging or interfering with a computer system; 3) Making, selling, distributing or possessing software for committing crimes; and 4) Accessing a computer system without authorization.[6]

In 2004 the Telecommunications (Interception Capability) Act was passed. The Act is lawful access legislation that allows law enforcement agencies to intercept online communications lawfully and requires network operators to be capable of intercepting online communications at the request of police. New Zealand is engaged in discussions with other members of the Quintet about the harmonization of their cyber-laws.

Role of the Private Sector – For-Profit

New Zealand's official cyber-security strategy highlights cooperation with the private sector in order to improve national responses to cybercrime, but it is short on details. Cooperation with internet service providers is suggested. Currently, New Zealand's largest telecommunications provider, Telecom New Zealand, offers internet subscribers retail licenses for commercial anti-virus software but has not detailed any broader initiatives.

The strategy also notes that the country is exploring ways to work with industry to support the enhancement of protection and computer security of critical national infrastructure from cyber-based threats; although, this initiative appears to be in the early stages as well. A review of major industry associations such as the New Zealand Bankers' Association, Internet Service Providers Association of New Zealand, and New Zealand Computer Society shows no articulation of efforts to combat cybercrime.

Role of the Private Sector – Not-For Profit

Partnership of the public and private, not-for profit sector is an element of the New Zealand approach. NetSafe is an independent, non-profit organization that has undertaken a number of initiatives.[7] Among these are the creation of a national cyber-bullying taskforce, advice and support for victims of telephone scams, development of consumer advice around smartphones and the delivery of cyber-safety education and awareness programs in schools. Another initiative is the Orb, a website for reporting online "problems" – crimes as well as

[6] New Zealand Police, *Electronic Crime Strategy to 2010 – Policing With Confidence*, 2007 New Zealand Government at http://www.police.govt.nz/resources/2007/e-crime-strategy/e-crime-strategy.pdf.
[7] NetSafe, *NetSafe: Cybersafety and Security advice for New Zealand,* at http://www.netsafe.org.nz.

objectionable material, privacy breaches and other online issues.[8] The Orb's public partners include New Zealand's police, the Department of Internal Affairs, the Privacy Commissioner, the Ministry of Consumer Affairs, the Commerce Commission, the National Cyber Security Centre and the New Zealand Customs Service.

Cooperation with other jurisdictions

New Zealand is cooperating with members of the Anglosphere as discussed above. The Anglosphere as a whole, and New Zealand specifically, as part of its strategy, are exploring joining the Council of Europe Budapest Convention on Cybercrime. New Zealand has come under criticism for the activities of Tokelau (three New Zealand atolls north of Samoa), which gives away its .tk domain name under an agreement with a Dutch company in exchange for free broadband services, and in so doing enables criminals to launch phishing attacks.[9]

Australia

Overview

Australia is following a strategy for cyber-security published in 2009 with the following priorities: improving threat awareness and response for national-interest systems; educating and empowering Australian individuals online; creating public-private partnerships to promote cyber-security; protecting government systems; engaging internationally; maintaining effective law enforcement; and developing a skilled workforce.[10]

In 2011, Australia announced it would develop a strategy for cyberspace in general.[11] This strategy will address online consumer protection, cyber-safety, cybercrime, cyber-security and cyber-defence. It will contemplate the creation of an Australian cyber-security czar or a cyber-security ombudsperson. The new strategy will be led by the Department of Prime Minister and Cabinet, a fact that reflects the increasing importance of cyber-security within Australia's national agenda. The roles of the private and public sectors under the current strategy are described below.

[8] The Orb, *The orb: reporting online crime, online*, at http://www.theorb.org.nz.
[9] Michael Field, "New Zealand territory world leader in cybercrime," Stuff at http://www.stuff.co.nz/technology/digital-living/4936881/New-Zealand-territory-world-leader-in-cybercrime (accessed 24 November 2011).
[10] Attorney-General's Department, "Cyber Security," Australian Government at http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity (accessed 27 November 2011).
[11] Department of the Prime Minister and Cabinet, "The Cyber White Paper: Connecting With Confidence," Australian Government at http://www.dpmc.gov.au/national_security/cyber_white_paper_factsheet.cfm (accessed 24 November 2011).

Role of the Public Sector – Policy

The lead policy public agency is the Attorney General (AG)'s Department.[12] This department chairs an interdepartmental committee on Cyber Security Policy and Coordination, through which it develops cyber-security policy for Australia. This committee determines priorities for the Australian Government, coordinates policy responses to cyber-security events, and coordinates cyber-security policy internationally. Therefore, government takes a leading role under the strategy for cyber-security, and the choice of the AG as the leading department focuses the strategy on legal issues.

Other important public sector bodies are Australia's Computer Emergency Response Team,[13] located within the AG's department, and Australia's Cyber Security Operations Centre, located within the Department of Defence. Both work with a range of other agencies, such as the Communications and Media Authority, the Australian Federal Police, the Australian Security Intelligence Organization, the Defence Signals Directorate, the Department of Broadband, Communications and the Digital economy, and the Information Management Office, to implement the strategy for cyber security.

These agencies collaborate through a model known as Joint Operating Arrangements. The agencies identify and analyze cyber-events of serious national consequence. The Joint Operating Arrangement determines which agency has the primary responsibility to respond and manage each specific event based on the nature of the event and the mandate of the agency.

Within the government, the strategy has led to the development of OnSecure, a central source for the Australian public sector to learn about and report on potential threats and vulnerabilities.[14]

Role of the Public Sector – Law

Australia has passed several pieces of legislation in order to create a cyber-security legal framework. The Cybercrime Act was passed in 2001 (amending the Criminal Code), the Spam Act in 2003 and the Surveillance Devices Act was passed in 2004. Under the existing strategy the government has introduced further legislation, the Cybercrime Legislation Amendment Bill 2011, mainly to facilitate lawful access, through proposed amendments to the Telecommunications (Interception and Access) Act of 1979.[15]

Further public sector law-related measures promoted under the strategy include providing additional resources for security and law enforcement agencies, ensuring effective communications between traditional and cyber branches of law enforcement to combat organized

[12] Attorney-General's Department, "Cyber Security," Australian Government at http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity (accessed 27 November 2011).
[13] CERT Australia, *Home,* Australian Government at http://www.cert.gov.au.
[14] OnSecure, *OnSecure Public Site – Unclassified*, Australian Government at http://www.onsecure.gov.au.
[15] Josh Taylor, "Tougher cybercrime laws hit parliament," ZDNet AU at http://www.zdnet.com.au/tougher-cybercrime-laws-hit-parliament-339317207.htm (accessed 24 November 2011).

cybercrime through the establishment of the Commonwealth Organized Crime Strategic Framework, educating legal professional with technological knowledge, and harmonizing Australia's legal framework with other jurisdictions. The proposed 2011 bill is intended, in that regard, to allow Australia to accede to the Council of Europe Convention on Cybercrime.[16]

Role of the Private Sector – For-Profit

The establishment of the Computer Emergency Response Team has created a role for the for-profit private sector. The sector is expected to share information and coordinate responses with the response team. Commercial internet service providers have developed a voluntary code of best practices around cyber-security and are also collaborating with the Australian government through the Australian Internet Security Initiative.[17] This initiative addresses the problem of compromised computers (colloquially known as 'zombies' or 'bots'). The initiative provides data about such computers to the participating businesses, which then inform their customers so that they will take steps to repair their computer.

The Critical Infrastructure Protection Program is another public-private partnership.[18] It operates across several sectors and allows owners and operators of critical infrastructure to work together and share information on common threats and vulnerabilities. The program addresses financial, communications, energy, food chain, health, transportation and water sectors. It is supplemented by the Critical Infrastructure Protection Modeling and Analysis program. The modeling and analysis program is in essence a computer model of how threats and vulnerability in one sector affect the others.

Role of the Private Sector – Not-For Profit

The not-for profit sector plays a relatively minor role within Australia's strategy. Once prominent cyber-security bodies, such as AusCERT,[19] a not-for profit computer emergency response team, have been subsumed by governmental bodies such as the Australian Computer Emergency Response Team discussed above. Public education and awareness initiatives are generally led by government and not by the not-for profit sector. For example, Stay Smart Online, a source of cyber-security information, is maintained by the government.[20] Similarly, Australia's Cyber Safety Plan is led by the Department of Broadband, Communications and the

[16] The Parliament of the Commonwealth of Australia, *Report 116 – Chapter 11: Council of Europe Convention on Cybercrime*, March 2011, Australian Government at http://www.aph.gov.au/house/committee/jsct/1march2011/report/chapter11.pdf.
[17] Australian Communications and Media Authority, "Australian Internet Security Initiative," Australian Government at http://www.acma.gov.au/WEB/STANDARD/pc=PC_310317 (accessed 24 November 2011).
[18] Trusted Information Sharing Network for Critical Infrastructure Resilience, *Home*, Australian Government at http://www.tisn.gov.au.
[19] AusCERT, *AusCERT – Australia's Leading Computer Emergency Response Team*, at http://www.auscert.org.au.
[20] Stay Smart Online, *Home,* Australian Government at http://www.staysmartonline.gov.au.

Digital Economy, with its major outreach initiative, CyberSmart, led by the Australian Communications and Media Authority.[21]

One prominent initiative for the not-for profit sector is the National Security Science and Innovation Strategy. This strategy aims to enhance the application of science and innovation to national security. The Australian government will allocate resources annually to researchers, entrepreneurs and funding programs on the basis of clearly defined national security objectives. Universities and research institutions play a major role within this initiative and conduct funded research in areas such as quantum cryptography and behavioural change.

Cooperation with other jurisdictions

Australia's approach is to forge bilateral or multilateral agreements with key allies and other likeminded nations. Australia is cooperating closely with other members of the Anglosphere and the UK in particular in this regard. The strategy calls for cooperation with other countries and within other international bodies as well. As discussed above, Australia has introduced legislation that will allow it to join the Council of Europe Convention on Cybercrime. Australia also participates in cyber-security specific international forums such as the Forum of Incident Response and Security teams and the International Watch and Warning Network.

Australia has indicated an interest in a coordinated global approach to combating cyber-security threats, and in international engagement, but it has not yet engaged countries from which threats are said to originate.

The United Kingdom

Overview

The UK released its latest cyber-security strategy in late 2011.[22] The strategy aims to achieve four objectives by 2015: establishing the UK as one of the most secure places in the world to do business in cyberspace; increasing the resiliency of the UK to cyber-attacks; shaping an open, stable and vibrant cyberspace for the public; and possessing the necessary knowledge, skills and capability to secure cyberspace.

The strategy places emphasis on the role of the private for-profit sector, which is discussed below. Previous strategies have come under criticism for the lack of cooperation between the government and the private sector.[23] Moreover, previous strategies have been criticized for being

[21]Cybersmart, *Cybersmart – Internet and mobile safety advice and activities*, Australian Communications and Media Authority at http://www.cybersmart.gov.au.
[22] Cabinet Office, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*, November 2011, UK Government at http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf.
[23] Tom Espiner, "UK cyber-readiness is 'patchy', says Chatham House," ZDNet UK at http://www.zdnet.co.uk/news/security-threats/2011/09/15/uk-cyber-readiness-is-patchy-says-chatham-house-40093946/ (accessed 1 December 2011).

short on financial resources and short-termed, with several government agencies, such as the National Drugs Intelligence Unit, leading to the National Criminal Intelligence Service, leading to the National Hi-Tech Crime Agency, leading to the Serious Organized Crime Agency, being created only to be replaced, under this strategy, by the National Crime Agency.[24]

Role of the Public Sector – Policy

The strategy creates a £650 million, National Cyber Security Program. The lead government office on the strategy is the Office of Cyber Security and Information Assurance in the Cabinet Office, under the oversight of the Minister for the Cabinet Office.[25] The office provides strategic direction and coordinates action related to enhancing cyber-securityand information assurance in the UK. Another key operational body is the Cyber Security Operations Centre that has operational responsibility for liaising with other governmental agencies in order to advance the program.

A key role for the public sector in the strategy will be to educate the public and to increase awareness of cybercrime. The UK has cited the lack of trained cyber-security professionals as an on-going challenge of combating cybercrime. The UK is looking to establish certified specialist training programs by March 2012, enhance postgraduate education in the field and develop a coherent, cross-sector research agenda to strengthen the UK's cyber academic base. The government would also like to be the single authoritative point of advice and source of best practices for the public.

As mentioned above, a National Crime Agency will be established with a National Cybercrime Unit within it. The agency will be responsible for organized crime, border policing, economic crime and child exploitation. The National Cybercrime Unit will be responsible for all cybercrime and for all crime-facilitating cyber-activity. The agency is slated to begin operations in 2013. A similar, existing body created under the previous strategy is the Police Central e-crime Unit.[26] This unit was staffed and funded by the private sector,[27] and was also intended to provide a national response to cybercrime. However, it does not deal with economic crime or child exploitation. The future of this unit is not clear under the new strategy.

In addition, the UK has a Computer Emergency Response Team.[28] The UK team works with teams of other nations as well as the Centre for the Protection of National Infrastructure, which

[24] Stuart Sumner, "UK's cyber crime defences come under fire," Computing at http://www.computing.co.uk/ctg/analysis/2106832/uk-s-cyber-crime-defences (accessed 1 December 2011).
[25] Cabinet Office, "Office of Cyber Security and Information Assurance (OCSIA)," UK Government at http://www.cabinetoffice.gov.uk/content/office-cyber-security-and-information-assurance-ocsia (accessed 3 December 2011).
[26] Metropolitan Police, *PCeU - Police Central e-crime Unit*, UK Government at http://www.met.police.uk/pceu/.
[27] Nick Heath, "E-crime police see UK firms pledging techies' time," ZDNet UK at http://www.zdnet.co.uk/news/security-management/2009/01/20/e-crime-police-see-uk-firms-pledging-techies-time-39597071/ (accessed 3 December 2011).
[28] GovCertUK, *GovCertUK*, UK Government at http://www.govcertuk.gov.uk/.

coordinates the UK's response activity to electronic attacks against critical national infrastructure.[29]

Role of the Public Sector – Law

As mentioned above, a main objective of the proposed National Crime Agency is to bring together existing law enforcement capability on cybercrime and to formalize the role of "white-hat" hackers. The strategy also aims to improve local police response, to encourage the courts to use existing powers to impose online sanctions for online offences, and to make reporting cybercrime easier. Victims are currently referred to a number of agencies such as Action Fraud, Consumer Direct and the Medicines and Healthcare Regulatory Agency, depending on the nature of the crime.

The UK amended its Computer Misuse Act in 2008, increasing penalties for hacking to enable requesting the extradition of hackers under existing treaties, and allowing for information to be shared with the private sector as discussed in the following section. Other important pieces of legislation are the Fraud Act 2006, the Proceeds of Crime Act 2002, the Anti-Terrorism, Crime and Security Act 2001 and the Communications Act 2003.

The government will consider whether sentences for online crimes are appropriate given the scale of most attempts. Attempts will be made to seize cyber-criminal assets, when possible. It is easier in the UK to succeed in private legal action for cybercrime as torts are based on trespass to property (namely, a computer), where financial damages are not required, rather than on fraud as in other jurisdictions.

Law enforcement and prosecution personnel will continue to be trained in cybercrime and updated with the latest technological developments. UK prosecutors are part of the Global Prosecutors E-Crime Network, established by the International Association of Prosecutors. The network encourages enhanced international cooperation and enables all jurisdictions to develop a coordinated approach, based on the Council of Europe Convention on Cybercrime.

Role of the Private Sector – For-Profit

A large emphasis in the current strategy is placed on the private sector, with the UK seeking to leverage private sector expertise for economic growth and export. The UK aims to promote itself as a safe haven in cyberspace, and draw business to the UK. The cyber-security strategy is intended to create a market in cyber-security services for UK businesses around the world, since they will have proven their strength in securing the UK domestic market.

Greater cooperation between the public and private sectors is envisioned as part of the strategy, both with the businesses that manage the government's own data, and with the private sector in general, to share information on threats in cyberspace. A joint public-private sector 'hub',

[29] Centre for the Protection of National Infrastructure, *CPNI* Website, UK Government at http://www.cpni.gov.uk/.

building on successful information-sharing between banks and the police, has recently begun a pilot program with five business sectors: defence, finance, communication, pharmaceuticals, and energy. Businesses will be expected to share such information with their competitors as well. Internet service providers are called on to support their customers and help them identify, address, and protect themselves from cybercrime.

The private sector is also expected to develop its own standards and indicators of good cyber-security products and services. The professional sector – insurers, auditors, and lawyers – will be required to promote better management of cyber-risks to its clients. Some examples of this cooperation are the private sector contribution to the Association of Chief Police Officers Good Practice Guide for Computer-Based Electronic Evidence,[30] and Get Safe Online, a joint initiative between government, law enforcement, and the private sector.[31] Get Safe Online provides independent, user-friendly information on dealing with various aspects of cybercrime, from malware to identity theft, and allows computer users and small businesses to use the internet more safely and securely.

The UK is also focused on enhancing the cooperation and security of Small and Medium Enterprises (SMEs). The strategy sets procurement targets of at least 25% of the value of government cyber-security contracts to go to SMEs, and is exploring a government-sponsored venture capital model to support SME innovation on cyber-security.

Role of the Private Sector – Not-For Profit

The not-for profit sector plays a relatively minor role in the new UK strategy. One example is the UK Council for Child Internet Safety, a partnership between government, industry, law enforcement, academia and NGOs that works to keep children and youths safe online. Another is the Warning, Advice and Reporting Point (WARP)[32], which is a community-based service where members can receive and share up-to-date advice on information security threats, incidents and solutions. The WARP operator decides what cyber-security information is relevant, delivers it to the community, facilitates the sharing of advice and best practices, and builds trust within the community, so that members report incidents to each other. WARPs will now be developed for the Public Sector as well.

The not-for profit sector also plays a role in training qualified cyber-security professionals through Cyber Security Challenge UK, a venture that partners with government, businesses, trade organizations and academics to recruit talent into the cyber-security profession.

[30] 7Safe, *Good Practice Guide for Computer-Based Electronic Evidence*, 2007, Metropolitan Police Service at http://www.met.police.uk/pceu/documents/ACPOguidelinescomputerevidence.pdf.
[31] Get Safe Online, *Get Safe Online: Home*, at http://www.getsafeonline.org/.
[32] Warning, Advice and Reporting Point, *Homepage | Warp.gov.uk*, UK Government at http://www.warp.gov.uk/.

Cooperation with other jurisdictions

The UK has ratified the Council of Europe (Budapest) Convention on Cybercrime and will work to persuade other countries to develop compatible laws. The strategy aims to establish internationally-agreed 'rules of the road' on the use of cyberspace, to ensure cooperation on cross-border law enforcement, and to develop practical confidence-building measures with other countries.

In addition to the Budapest Convention the UK is also part to NATO's cyber-defence policy, adopted in 2011. The policy identifies cyber-attacks as a key threat for which NATO defensive capability should be developed. The UK rejected a Russian proposal for a global treaty on cybercrime because it was seen as inferior to the Budapest Convention. The UK has been party to several bilateral declarations establishing joint frameworks on cybercrime, with Australia, France and the US.

The strategy is aware of the difficulties of pursuing international cooperation in cyberspace, and acknowledges that the application of existing legal principles to cyberspace is not uniform, since appropriate legislation does not exist in all countries. Perhaps for that reason the strategy concentrates on creating a lead role for the UK in cyber-security and in cooperation with "like-minded" jurisdictions, according to the 2011 London Conference on Cyberspace.[33]

The United States

Overview

The United States is focused both on the military aspect of cyber-security and on international cooperation in order to enhance cyber-security. The US released two strategies in 2011: the Department of Defense Strategy for Operating in Cyberspace,[34] and the International Strategy for Cyberspace.[35] The Department of Defense has set up a prominent military command – the Cyber Command, which will execute the US's military strategy.[36] The military strategy has five initiatives: to treat cyberspace as an operational domain, to employ new defence operating concepts, to partner with other US government departments and the private sector, to build robust relationships with US allies and international partners, and to leverage the US's ingenuity.

The International Strategy has seven "action lines" on which the US is seeking international cooperation: e-commerce, cyber-security, legal, military defence, internet governance,

[33] Foreign & Commonwealth Office, "Conference on Cyberspace," UK Government at http://www.fco.gov.uk/en/global-issues/london-conference-cyberspace/ (accessed 3 December 2011).
[34] US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, US Government at http://www.defense.gov/news/d20110714cyber.pdf.
[35] White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011, US Government at http://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf.
[36] US Strategic Command, "U.S. Strategic Command – U.S. Cyber Command," US Government at http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed 5 December 2011).

international development, and internet freedom. The US aims to act on these items through diplomacy, international development and defensive collaboration.

Role of the Public Sector – Policy

The lead policy office for the US is the White House Cyber-security Coordinator, colloquially known as the cyber-security "Czar". The cyber-czar was established to coordinate the work of the many federal agencies that were established within individual departments, and to counter the criticism that US cyber-security was suffering as a result.

For example, the Department of Justice, Department of State and Department of Commerce all host civilian agencies responsible for cyber-security and fighting cybercrime. Other agencies are located within the Department of Homeland Security, such as the National Cyber-security and Communications Integration Center, which coordinates cyber incident response efforts within the US government, the US Computer Emergency Response Team, the FBI Cyber Crime Task Force and the FBI Internet Crime Complaint Center. The Department of Defense, in addition to the military's Cyber Command, also hosts the NSA, and the Cyber Crime Center, which sets the standards of digital evidence processing, analysis, and diagnostics.

Under the 2011 international strategy, many of these agencies that have traditionally had a domestic focus will look to collaborate with similar international partners.

The National Initiative for Cyber-security Education is coordinated by the US National Institute of Standards and Technology. There are four education tracks: increasing general cyber-security awareness for the public; formal cyber-security education in K-12, higher education and vocational programs; improved recruitment, development and retention of skilled public sector employees in cyber-security; and cyber-security training and professional development required for government civilian, military, and contractor personnel.

Role of the Public Sector – Law

The US is currently in the process of updating several pieces of federal, cybercrime-related legislation. Ultimately, as part of its international strategy, the US would attempt to ensure that similar legislation exists around the world. Among the updated statutes and regulations are the Computer Fraud and Abuse Act, the Homeland Security Act, the Cyber-security Regulatory Framework for Covered Critical Infrastructure, the Federal Information Security Management Act and the Cyber Intelligence Sharing and Protection Act, discussed below. In addition to updated legislation, a bill currently in the US Senate's Committee on Foreign Relations proposes to require an annual report to Congress on foreign cybercrime against the US government, industry and individuals, along with efforts to prevent and persecute cybercrime by foreign countries and multilateral organizations.

Within the US Justice Department, the Computer Crime and Intellectual Property Section is responsible for enforcing the Computer Crime Initiative, a program designed to combat cyber-attacks on critical information systems. It is illuminating to note that the US combines cybercrime with IP protection – a factor that has made cooperation more difficult with other jurisdictions that do not share this view. The US Secret Service made approximately 1,200 cybercrime-related arrests in 2010.[37]

As part of its international emphasis, the US has also contributed to legislative development. The American Bar Association was the lead contributor for the International Telecommunications Union's (ITU) *Toolkit for Cybercrime Legislation*, based largely on the Convention on Cybercrime and relevant legislation for developed countries.[38]

Role of the Private Sector – For-Profit

Similar to the UK, the US is realizing that the for-profit sector needs to play a major role in cyber-security given the experience and resources that the sector has, including the expertise the sector provides governments for their own computer and network infrastructure. For example, Microsoft's Digital Crimes Unit disables botnets, and Microsoft has launched lawsuits against non-US citizens in US courts against individuals in control of botnets.[39] Internet security companies have released regular cybercrime reports; although, these reports have faced some criticism for being primarily driven by commercial interests and perhaps overstating cybercrime threats.

In an effort to improve communication between government and the private sector, the Cyber Intelligence Sharing and Protection Act was introduced in 2011 in order for US intelligence agencies to be able to share classified cyber-threat information with approved US companies, while encouraging companies to share their own information with the government or other companies.[40]

The for-profit sector also educates public sector professionals on cybercrime. Symantec launched the Norton Cyber-security Institute,[41] which amongst other initiatives plans to offer

[37] Department of Homeland Security, "Statement of Assistant Director A.T. Smith, United States Secret Service, before the House Committee on Financial Services, Subcommittee on Financial Institutions and Consumer Credit, 'Cybersecurity: Threats to the Financial Sector,'" US Government at http://www.dhs.gov/ynews/testimony/20110914-smith-threats-to-financial-sector.shtm (accessed 5 December 2011).
[38] Telecommunication Development Sector, *ITU Toolkit for Cybercrime Legislation*, February 2010, International Telecommunications Union at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf.
[39] Ryan Naraine, "Microsoft kills botnet that hosted MacDefender scareware," ZDNet US at http://www.lunarsoft.net/featured/microsoft-kills-macdefender-scareware-botnet (accessed 1 December 2011).
[40] US Government Printing Office, *H. R. 3523*, 30 November 2011, US Government at http://www.gpo.gov/fdsys/pkg/BILLS-112hr3523ih/pdf/BILLS-112hr3523ih.pdf.
[41] Norton from Symantec, "Norton Unveils Global Initiative to Combat Cybercrime," Symantec Corporate, http://www.symantec.com/about/news/release/article.jsp?prid=20110504_01 (accessed 28 November 2011).

a two day, bi-annual course for US state AGs pursuing cybercrime cases, in collaboration with the National Center for Justice and the Rule of Law at the University of Mississippi Law School.[42]

Role of the Private Sector – Not-For Profit

A proposal similar to the Cyber Intelligence Sharing and Protection Act contemplates information sharing through the not-for profit sector by creating a not-for profit National Information Sharing Organization.[43] This organization would facilitate the collection and distribution of information on cyber-threats shared among the federal government, state and local governments, private companies and education institutions.

The National Cyber-Forensics and Training Alliance is a not-for profit organization composed of representatives of industry and academia. The alliance, in cooperation with the FBI, helps protect US critical infrastructure by participating in cyber-forensic analysis, tactical response development, technology vulnerability analysis, and the development of advanced training.

The National Cyber Security Alliance is a not-for profit private-public partnership that delivers education and knowledge building efforts for personal, work and school internet users. This alliance runs the Stay Safe Online website, providing information to keep users and their organizations, networks, and sensitive information safe online and encourage a culture of cyber-security.[44]

Carnegie Mellon's Computer Emergency Response Team was created in 1988. The university not only helped the Department of Homeland Security to create the US response team, but has also worked to build a network of more than 50 computer security incident response teams internationally, including the Canadian Cyber Incident Response Centre. The program provides a trusted, 24-hour, single point of contact for emergencies and works with a number of stakeholders to research and develop protocols and technologies used to counter large-scale, sophisticated cyber threats.[45]

Cooperation with other jurisdictions

The release of a cyber-security strategy dedicated to international cooperation demonstrates the large emphasis the US places on cooperating with other jurisdictions. The US

[42] The Norton Cyber-security Institute also plans to sponsor the Canadian not-for profit Society for the Policing of Cyberspace's international anti-cybercrime law enforcement training programs for investigators.
[43] Committee on Homeland Security, *DISCUSSION DRAFT: To amend the Homeland Security Act of 2002 to make certain improvements, in the laws relating to cybersecurity, and for other purposes*, 2 November 2011, US Government at http://homeland.house.gov/sites/homeland.house.gov/files/Draft%20Legislative%20Proposal%20on%20Cybersecurity.pdf.
[44] Stay Safe Online, *Stay Safe Online | Brought to you by the National Cyber Security Alliance*, at http://www.staysafeonline.org/about-us/about-national-cyber-security-alliance.
[45] CERT, *Welcome to the CERT Program*, Carnegie Mellon University at http://www.cert.org/.

was an original signatory to the Council of Europe's Convention on Cybercrime and ratified the treaty in 2006 – currently, the only non-member state to do so. The US is actively promoting adoption of the Convention of Cybercrime with other countries, and using it as a basis for domestic cybercrime legislation in order to harmonize laws across jurisdictions.

The US also established a working group on cyber-security and cybercrime with the EU in 2010 to address emerging threats to global networks.[46] Further European and US cooperation is evidenced by NATO's cyber-defence policy adopted on June 2011.

The US continues to work closely with its traditional Anglosphere allies, reaffirming UK-US cooperation on cyberspace in 2011. Cyber-security cooperation was a key part of an updated US-Australia defense treaty to help combat cyber threats in the Pacific region. In addition to more defence-focused cyber-security, the FBI was a key instigator of the Strategic Alliance Cyber Crime Working Group that is looking to increase ties between law enforcement of the US, UK, Canada, Australia and New Zealand.

The released international strategy emphasizes capacity building in developing and newly industrialized states. In 2011, the US donated forensic equipment and software to help modernize the capabilities of the Anti-Transnational and Cyber Crime Division of the Philippine National Police.[47] The US has also provided funding and training to countries like Romania, which has a thriving cybercrime industry. To facilitate joint cybercrime investigations involving Romania and the US, the FBI has an agent embedded within the Organized Crime Directorate of the Romanian Police, as well as several other countries.[48] Also in 2011, the US and India signed a Memorandum of Understanding to exchange critical cyber-security information and best practices between the US and Indian computer emergency response teams.[49]

[46] EU-US Justice and Home Affairs Ministerial, "Cyber security: EU and US strengthen transatlantic cooperation in face of mounting global cyber-security and cyber-crime threats," European Union, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/246 (accessed 5 December 2011).
[47] Aaron B. Recuenco, "US aid bolsters PNP anti-cyber crime drive," Manila Bulletin Publishing Corporation at http://www.mb.com.ph/articles/339429/us-aid-bolsters-pnp-anticyber-crime-drive (accessed 5 December 2011).
[48] Gordon M. Snow, "Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism," Federal Bureau of Investigation, http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism (accessed 6 December 2011).
[49] The Economic Times, "India, US join hands to fight cyber crime, sign MoU," India Times at http://articles.economictimes.indiatimes.com/2011-07-19/news/29790778_1_cyber-security-cert-fight-cyber (accessed 6 December 2011).

Europe

Space precludes a detailed discussion of the strategic approach of the European Union and all its Member States, or of the approaches of other European countries. Instead, three Member States – Germany, France and Romania, as well as the Baltic States, were chosen to illustrate the wide range of approaches that exists within Europe itself.[50]

Germany

Overview

Germany has been identified as a major target of cybercrime in Europe, suffering from a large number of bot infections.[51] At the same time, Germany has been critiqued for not providing additional funds for cyber-security and protection and having too decentralized cyber response structure to provide efficient security. Germany possesses a large number of public and private (both for-profit and not-for profit) computer emergency response teams that could benefit from enhanced cooperation along with ongoing efforts to coordinate between the private sector and state agencies.[52]

Germany published its Federal Cyber Security Strategy in early 2011. The Federal Government will specifically focus on ten strategic areas: critical information infrastructures; IT systems security; public administration of IT security; a National Cyber Response Centre (NCZA); a National Cyber Security Council; effective crime control extended into cyberspace; coordinated action on cyber-security in Europe and worldwide; use of reliable and trustworthy IT; personnel development in federal authorities; and tools to respond to cyber-attacks.[53]

Role of the Public Sector – Policy

The Federal Ministry of the Interior (BMI) is the coordinating government authority for Germany's cyber-security policy but several other ministries play a critical role. The NCZA, created in 2011, reports to the Federal Office for Information Security (BSI) and cooperates with a number of relevant agencies covering law enforcement, military, critical infrastructure regulators and privacy protection agencies. The NCZA is tasked with evaluating cyber-attacks and developing defences and coordinating the necessary measures to disable the threat. The Federal Criminal Police Office (BKA), which works with the NCZA, also provides preventive measurements against cybercrime and works closely with the BSI on cybercrime topics.

---

[50] The Baltic States are discussed further in the report after the CIS countries.

[51] "Germany tops European cybercrime list," automotiveIT International at http://www.automotiveit.com/germany-tops-european-cybercrime-list/news/id-002337 (accessed 21 December 2011).

[52] Arne Schönbohm, "Germany Must Defend Against Cyber Attacks," Atlantic Initiative, http://www.atlantic-community.org/index/articles/view/Germany_Must_Defend_Against_Cyber_Attacks_ (accessed 21 December 2011).

[53] Federal Ministry of the Interior, *Cyber Security Strategy for Germany*, February 2011, German Government at http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber_eng.pdf?__blob=publicationFile.

In 2009, the Bundestag passed the Act to Strengthen the Security of Federal Information Technology. The act made the BSI the central reporting office for cooperation among federal authorities in matters related to protection against malicious software and threats to federal communications technology, destruction of personal data, and warnings of IT security vulnerabilities. The government also maintains a number of emergency response teams overseen by the BSI and the Ministry of Defence.

The BMI published the German National Strategy for Critical Infrastructure Protection in 2009. It is carried out jointly by government bodies such as the Federal Office of Civil Protection and Disaster Assistance, the BSI and Federal Network Agency and the private sector. In addition to government coordination with large private sector actors, the BMI and the Federal Ministry of Economics and Technology launched an initiative to raise awareness of internet security in SMEs to improve the competitiveness those companies.

Germany was recently recognized in a report commissioned by a US intelligence contractor as having the leading legal and regulatory framework among the countries surveyed, in part for being one of only five countries to have a comprehensive national cyber plan and a comprehensive cybersecurity plan.[54]

Role of the Public Sector – Law

Cybercrimes are generally addressed by updates to the German Criminal Code to explicitly criminalize traditional crimes committed by or to computers and networks. Relevant updates include additions to Violation Of Privacy (Section 202a Data espionage, 202b Phishing, 202c Acts preparatory to data espionage and phishing), Forgery (Section 269 Forgery of data intended to provide proof, 270 Meaning of deception in the context of data processing) and Criminal Damage (Section 303a Data tampering, 303b Computer sabotage, 303c Request to prosecute).

With a legal system that places a strong emphasis on privacy rights due to historical state abuses, the BMI is currently exploring new legislation to address data protection on the internet, geo-data services, and a right to claim immaterial damages. The government has come under some criticism for using malware for law enforcement purposes. While the narrow use of Trojans for wiretapping purposes was approved by German courts in 2008,[55] the software seems to have far more extensive capabilities that may leave the computer vulnerable to planting of evidence by law enforcement or third-party actors. Further, the data is thought to have been routed through US-based servers in a possible attempt to hide German authorities involvement.

[54] Economist Intelligence Unit, "Cyber Power Index: Findings and Methodology," Booz Allen Hamilton at http://www.cyberhub.com/Home/DownloadFindings (accessed 29 January 2012).
[55] Jason Mick, "German Hackers: Gov't Trojan Capable of Planting Evidence, Cybercrime," Daily Tech at http://www.dailytech.com/German+Hackers+Govt+Trojan+Capable+of+Planting+Evidence+Cybercrime/article22966.htm (accessed 21 December 2011).

Role of the Private Sector – For-Profit

The for-profit sector is not as engaged in the national cyber-security strategy as it could, leading to criticism of the 2011 German approach which does not emphasize cooperation with the private sector. While the vast majority of German business executives believe cyber-attacks will increase in general, only 38% feel a specific threat to their firm.[56] In 2010, the German data protection authorities responsible for the private sector issued minimum requirements for the qualifications and independence of company data protection officers after inspections revealed a generally insufficient level of expertise to meet the Federal Data Protection Act. Further, changes in data processing volumes and complexity frequently increase the burden on data protection officers without a compensating increase in resources needed to ensure proper oversight.[57]

A number of German businesses operate computer emergency response teams including Siemens, Volkswagen, Telekom and Commerzbank. CERTCOM AG is the first commercial response team providing IT security products and services to manufacturing companies. In a coordinating effort, the Federal Association for Information Technology, Telecommunications and New Media (BITKOM) plays an important lobbying and coordinating effort for IT, telecommunications, and new media industries in Germany.

Role of the Private Sector – Not-For Profit

Non-profits largely appear to play a small but critical role in German cybercrime and cyber-securitypolicy. CERT-Verbund is an alliance of German public and private security and computer emergency response teams. Additionally, a number of academic institutions and independent think tanks provide research on broad areas related to cybercrime.

Cooperation with other jurisdictions

Germany was an original signatory to the Budapest Cybercrime Convention, with ratification occurring in 2009. In order to better coordinate legal frameworks and technical capabilities, Germany is looking to work with multinational organizations such as the United Nations, the EU, the Council of Europe, NATO and others. The aim is to ensure the coherence and capabilities of the international community to protect cyberspace.[58]

Germany is also exploring operation methods of better international cooperation with law enforcement agencies. In 2010, it joined several other countries – including the UK and Australia – in an internship program with the US's National Cyber-Forensics & Training Alliance.

---

[56] Rolf Wenkel, "Executives underestimate cybercrime danger," Deutsche Welle at http://www.dw-world.de/dw/article/0,,15083403,00.html (accessed 21 December 2011).
[57] European Network and Information Security Agency, *Germany Country Report*, May 2011, European Union at http://www.enisa.europa.eu/act/sr/files/country-reports/Germany.pdf/view.
[58] Federal Ministry of the Interior, *Cyber Security Strategy for Germany*, February 2011, German Government at http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber_eng.pdf?__blob=publicationFile.

Furthermore, the country works with the European Government computer emergency response team. In addition to multilateral initiatives, Germany has cooperated bilaterally via the Franco-German Council of Ministers on issues including strengthening the protective measures against cyber-attacks.

However, Germany may have some reservations about international cooperation and extra-jurisdictional enforcement.[59] Germany – along with France and the UK – raised concerns that a centralized EU cybercrime agency may conflict with national law enforcement efforts.

France

Overview

The current French cyber-security policy is highly influenced by the release of the 2008 White Paper on Defence and National Security. An update for 2012 is being developed and expected to focus on four major topics: larger strategic developments, alliances, cross-sector threats such as terrorism and cyber-attacks, and financial and economic crises. The 2008 version labelled the threat against critical infrastructure from cyber-attacks a national security concern and stated that France is pursuing a dual strategy of building its defensive and offensive capabilities to ensure French sovereignty is "expressed fully" in cyberspace.[60]

Role of the Public Sector – Policy

The key outcome of the 2008 White Paper was the creation of a French Network and Information Security Agency (ANSSI),[61] under the authority of the Prime Minister. The ANNSI is attached to the General Secretariat for Defence and National Security (SGDSN). The SGDSN comprises a permanent group of around 350 staff with a €100 million budget, which makes the secretariat a key influencer of policy.[62] The ANSSI was established in 2009 and its core missions are: the defence of sensitive government networks; the development of trusted products and services for government entities and economic actors; the support of government entities and critical infrastructure operators; and informing companies and the general public about information security threats through an active communication policy. The offensive counterpart for France's cyber-strategy operates under the Joint Staff, with both the army and the air force possessing electronic warfare units; intelligence services are also pursuing offensive

[59] ACM, "UK Minister, CoE chair Brokenshire+ to EuroFora on CyberCrime +CoE Internet Governance Strategy 2015," EuroFora at http://www.eurofora.net/newsflashes/news/coeinternetstrategy.html (accessed 21 December 2011).
[60] James A. Lewis and Katrina Timli, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*, 2011, United Nations Institute for Disarmament Research at http://www.unidir.ch/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf.
[61] Network and Information Security Agency, *The* ANSSI, French Government at http://www.ssi.gouv.fr/en/the-anssi/.
[62] Fabio Liberti and Camille Blain, "France's National Security Strategy," Real Instituto Elcano at http://www.realinstitutoelcano.org/wps/portal/rielcano_eng/Content?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/defense+security/dt3-2011 (accessed 28 January 2012).

capabilities.[63]

In 2011, the ANSSI released the official French cyber doctrine. France's four objectives in cyberspace are: being a global power in cyber defence; protecting information sovereignty to guarantee France's freedom of decision; securing critical infrastructure and maintaining privacy in cyberspace. Information sovereignty and international cooperation are emphasized.

In addition to the ANSSI's role in helping to secure infrastructure, France issued a 2006 decree on Critical Infrastructure Protection that required operators to submit a master plan to ensure compliance with national security guidelines. The French Ministry of Economy, Industry and Employment has responsibility to verify plans have been implemented properly and satisfactorily. France has also created an inter-ministerial body to coordinate telecommunication and internet network performance.[64] Further, the National Council of Digital Matters was created in 2011 under the Minister of the Digital Economy to inform the government on the issues related to the digital economy and to improve dialogue between the government and the internet private sector. France also operates a governmental Computer Security Incident Response Team, which is the point of contact for all computer-related security incidents regarding France.

Role of the Public Sector – Law

France is one of the earliest adopters of data protection legislation, passing the Information Technology and Liberty Act in 1978. Ten years later the French penal code was updated by introducing Articles 323-1 to 323-7, regarding intrusion of information systems. The penal code was updated several times since, including the Reinforcing Trust in the Digital Economy Act in 2004. The updates cover various cyber-related areas including fraud, the distribution of child pornography, and spam with specific provisions being introduced in the Penal Procedure Code as to encryption, communications monitoring, and data seizure.[65] Other relevant pieces of the regulatory framework include the eGovernment Act (2005) and the eCommerce Act (2004).

France also introduced a law promoting the distribution and protection of creative works on the internet in 2009, widely known as the HADOPI Law for the acronym of the government agency created, to encourage compliance with copyright laws. This legislation is known colloquially as the "three-strike" rule. The system relies on a graduated response of notices when a user's IP address has been identified as sharing infringing content online. After a third notice, the agency may have a hearing with the user and may then refer the matter for judicial review. If a judge

[63] James A. Lewis and Katrina Timli, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*, 2011, United Nations Institute for Disarmament Research at http://www.unidir.ch/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf.
[64] European Network and Information Security Agency, *France Country Report*, May 2011, European Union at www.enisa.europa.eu/act/sr/files/country-reports/France.pdf.
[65] European Network and Information Security Agency, *France Country Report*, May 2011, European Union at www.enisa.europa.eu/act/sr/files/country-reports/France.pdf.

decides punishment is merited, the user can be fined up to €1500 or lose their internet connection for up to one month. The law has been controversial, with digital rights activists and organizations like the UN and OSCE suggesting disconnection may be a disproportionate sanction.[66]

The Central Office for the Fight against Crime Related to Information Technology and Communication (OCLCTIC) is the lead cybercrime actor within French law enforcement. The agency was established in 2000 and its primary function is to facilitate and coordinate police activities against cybercrime at the national level and serve as the international contact point for cybercrimes. The OCLCTIC conducts investigations and assists national level civilian police, military police and fraud investigators, while also supporting local and regional police with IT expertise, IT data collection, and other IT crime-related needs. The OCLCTIC also houses a sub-unit, the Central Brigade for the Suppression of Counterfeit Credit Cards.

France was the recent victim of cyber espionage, when the Economy and Finance ministries were targeted for important G20 documents. Investigations by the ANSSI and the ministries' IT teams found the large-scale attack lasted for weeks before being detected and the level of technical expertise required suggested the attackers were organized professionals.[67] To help monitor cybercrime incidents on the internet, France has created the Pharos reporting platform, which allows the public to report suspicious websites or messages they encounter while surfing on the internet. In 2010, Pharos gathered over 77,000 reports that resulted in the investigation of between 6,000 and 8,000 incidents. 57% were related to fraud, 22% were classified as an offense against underage children, 10% were cases of "xenophobia" and 8% "others". Just 3% of the reports were classified as unfounded.[68]

France was an original signatory of the Budapest Convention on Cybercrime in 2001, as well an original signatory of the 2003 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.[69] France ratified both treaty and protocol in 2006.

Role of the Private Sector – For-Profit

The French for-profit sector appears to be more involved in attempts to combat intellectual property piracy than in other issues. The government provides the sector with

[66] Timothy B. Lee, "French copyright cops: we're swamped with "three strikes" complaints," Ars Technica at http://arstechnica.com/tech-policy/news/2011/07/french-agency-were-swamped-with-three-strikes-complaints.ars (accessed 20 February 2012).
[67] Network and Information Security Agency, "Cyber-attack against the French Ministries of Economy and Finance," French Government at http://www.ssi.gouv.fr/en/the-anssi/publications-109/press-releases/cyber-attack-against-the-french-ministries-of-economy-and-finance.html (accessed 28 January 2012).
[68] Francois Paget, "Responses to Cybercrime in Japan and France," McAfee Inc at http://blogs.mcafee.com/mcafee-labs/responses-to-cybercrime-in-japan-and-france (accessed 28 January 2012).
[69] Due to concerns about the potential impact on domestic freedom of speech laws in various countries, the protocol's subject matter was excluded from the original Convention on Cybercrime treaty.

subsidies that, critics claim, will enable the usage of private sector companies to conduct online surveillance and filtering.[70] In 2009, with the assistance of the National Institute of Industrial Property, efforts at self-regulating resulted in a French Charter on the Fight against Cyber-Counterfeiting between e-commerce platforms, industry associations and rights holders. The initiative has been made permanent and continues to expand signatories, now including ad networks and postal operators.

Role of the Private Sector – Not-For Profit

France operates a not-for profit organization called Signal Spam, a public-private partnership dedicated to eliminating spam. Signal Spam partners include law enforcement agencies, French ISPs, security firms, consumers and marketing unions. End users can report all forms of spam, both legitimate unwanted advertising and cybercrime threats such as scams, frauds, and phishing attempts to the Signal Spam database. Analysis of the database assists with botnet detection and the identification of other cybercriminals.

Two NGOs operate in France that focus on the online protection of children. Internet Sans Crainte is the French organization of the Safer Internet Program. Action Innocence, working with the Canton of Geneva's Department of Justice, Police and Safety and Department of Public Education, operates in all French-speaking parts of Europe.

Cooperation with other jurisdictions

As noted above, France has ratified the Convention on Cybercrime. France has also partnered with a number of countries on a bilateral basis, and participates in a number of other multi-lateral fora discussed below. France and Estonia signed a cooperation agreement in November 2010 that will see the French ANSSI and Estonian Informatics Centre share information and experience to help protect IT systems.[71] In 2010 France and Germany pledged to work together on improving cyber defences and ANSSI and the German BSI reinforced their efforts to cooperate against emerging forms of cyber-attacks.[72]

France is also an original partner with Ireland in the 2CENTRE project, Cybercrimes Centres of Excellence for Training Research and Education. The project, supported by the European Commission, is designed to partner academics, law enforcement officers and members of industry to develop the technical skills and education needed for cybercrime investigation. The University of Technology of Troyes and University of Montpellier are responsible for the French Centre of Excellence. While the initiative is quite new, it is expanding to other European

[70] "Countries Under Surveillance: France," Reporters Without Borders at http://en.rsf.org/surveillance-france,39715.html (accessed 10 February 2012).
[71] Network and Information Security Agency, "Cyberdefence: France and Estonia sign a cooperation agreement," French Government at http://www.ssi.gouv.fr/en/the-anssi/publications-109/press-releases/cyberdefence-france-and-estonia-sign-a-cooperation-agreement.html (accessed 28 January 2012).
[72] European Network and Information Security Agency, *France Country Report*, May 2011, European Union at www.enisa.europa.eu/act/sr/files/country-reports/France.pdf.

nations.[73]

France has also worked on enhancing cyber defences through participating in US-led cyber exercises, European cyber exercises and NATO's 2010 exercise. In addition to specific cyber exercises, France's emergency response team is an active member in the European Government group.

Romania

Overview

As Romania consolidates its transition to democratic governance and a market-based economy, it faces growing pains in its ICT policy – both technical and social. Often perceived as a cybercrime haven, the government is attempting to modernize telecommunication and internet infrastructure and working towards basic access issues for large parts of the country. While suffering from capacity issues, government and law enforcement officials are working with international counterparts in both the EU and US in an attempt to enhance cybercrime response.

Role of the Public Sector – Policy

Government remains the most important and active actor in developing a response to cybercrime. In 2009, the Romanian Government approved a Digital Romania Strategy, a national strategy proposed by the Ministry of Communications and Information Society (MCIS) for 2010-2013. The primary goals of the strategy are to modernize the state through improved, computerized interaction with citizens and businesses and move towards an information society and knowledge based society.

Under the umbrella of this digital strategy, the government is developing a unified strategic framework that includes the following strategic directions: network interoperability; IT infrastructure deployment; electronic government services; cybercrime; improved access; national strategy for postal services and telecommunications; and broadband and spectrum strategy. In addition to planning, the strategy looks to implement ICT infrastructure upgrades, improve governance and the implementation of a national centre for the prevention, detection and combating of cybercrime.[74] With funding in late 2010 from the European Commission, MCIS and an intergovernmental commission are studying how to develop and deploy the necessary infrastructure for a modern, robust ICT system that includes protection against cyber-attacks on critical national infrastructure.[75]

[73] 2Centre, *2CENTRE*, Cybercrime Centres of Excellence Network for Training Research and Education at http://www.2centre.eu/.
[74] Government, *Government's Program: Chapter 14 – Information Society*, Romanian Government at http://www.gov.ro/chapter-14-information-society__l2a1048.html (accessed 5 January 2012).
[75] European Network and Information Security Agency, *Romania Country Report*, May 2011, European Union at http://www.enisa.europa.eu/act/sr/files/country-reports/Romania.pdf/view.

While MCIS is the lead government body for cybercrime policy, the Service for Combating Cybercrime operating in the Romanian Directorate for Investigating Organised Crime and Terrorism Offences (DIICOT) is the competent Romanian authority in enforcing the legal measures against cybercrime. The DIICOT works closely with other national and international law enforcement agencies to combat domestic and international cybercrime. Romania created a national computer emergency response team in 2009 and established internal regulations the following year, though its impact at this time seems minimal. The Service for Countering the Cyber Criminality is also responsible for running e-Fraudo,[76] a centralized reporting point for various types of cybercrime from malware to phishing and other online frauds and online child exploitation.

Role of the Public Sector – Law

In Romania, cybercrime is primarily prosecuted under Law 161/2003, Anti-Corruption Law, Title III with some protections provided under Law 365/2002 Electronic Commerce. Additional regulatory elements include the Law on Free Access to Information of Public Interest (2001); the Law on the Protection of Persons concerning the Processing of Personal Data and the Free Circulation of Such Data (2001); and the Law on the processing of personal data and the protection of privacy in the electronic communications sector (2004). Romania was also an original signatory to the Budapest Convention, ratifying it in 2004.

Although Romania remains a perceived cybercrime haven, its government has shown an increased capacity for law enforcement, supported by increased international assistance. It has been estimated that 80-90% of internet fraud cases investigated by the police involve American businesses or individuals,[77] so a high level of US cooperation is understandable. In 2005, 153 cybercrime cases were investigated jointly by Romanian and US authorities;[78] this number climbed to 977 new cases registered during the first eight months of 2011 by DIICOT.[79] The climb is attributed not only to increased law enforcement, but also to a combination of social factors such as a lack of legitimate economic opportunities and lenient sentences.

Role of the Private Sector – For-Profit

Without a well-developed market-economy, the for-profit private sector in Romania plays a minor role in combating cybercrime. Telecommunication and internet service providers, in general, do not voluntarily report security incidents and operate under a number of codes of conduct. While there are a number of industry organisations currently in Romania (e.g. the

[76] Romanian Police, *Crime Information Service*, Romanian Government at http://www.efrauda.ro/.
[77] State Department, "FY 2007 U.S. Government Assistance to and Cooperative Activities with Central and Eastern Europe," US Government at http://www.state.gov/p/eur/rls/rpt/seedfy07/116209.htm (accessed 5 January 2012).
[78] State Department, "U.S. Government Assistance to and Cooperative Activities with Central and Eastern Europe," US Government at http://www.state.gov/p/eur/rls/rpt/92682.htm (accessed 5 January 2012).
[79] Lucian Constantin, "Romania's Anti-Cybercrime Efforts Lack a Social Component," CSO at http://www.csoonline.com/article/690521/romania-s-anti-cybercrime-efforts-lack-a-social-component (accessed 5 January 2012).

Romanian Association for Electronic and Software Industry, the National Association of Romanian ISPs, the Employers' Association of the Software Industry and Services, the Association for IT&C, the Association of Telecommunications Operators, Cable Communication Association), the European Network and Information Security Agency reports not much public information is available on the cooperation between the Romanian government, industry and other stakeholders on combating spam and malware.[80]

Role of the Private Sector – Not-For Profit

This sector plays a relatively minor role in tackling cybercrime in Romania. RoCSIRT is an outgrowth of the Computer Security Incident Response Team of the Romanian Education Network, a collective of academic institutions in Romania. Key stakeholders in the academia include the Military Technical Academy, National Communications Research Institute and National Institute for Research and Development in Informatics. In addition, the Information and Communication Technology association, the Romanian Association of Telecommunications' Engineers and the Association for Consumers' Protection all play a small contributing role in national information security.

Safer Internet is a collaborative project between NGOs, government and industry, with further funding from the European Commission. The website serves as a contact point for reports on online material of an illegal or harmful nature for children. In addition to the hotline, the site strives to provide teachers, parents and child protection specialists with knowledge and tools to protect their children in the new technological environment.[81]

Cooperation with other jurisdictions

Although it ratified the CoE Convention on Cybercrime early, Romania lacks the internal resources to tackle its cybercrime problem effectively on its own. As noted above, it has received EU funding to modernize Romanian ICT networks, and in 2010 participated in the first pan-European exercise on critical information infrastructure protection, Cyber Europe 2010, designed to test defense systems against cyber-attacks.

Further, Romanian law enforcement actors work closely with counterparts in the US and FBI officers are stationed in Romania to support joint investigations. Approximately 228 Romanian law enforcement officers have graduated from the FBI's International Law Enforcement Academy in Budapest and from the National Academy in the US, with another 350 officers taking specialized courses in the US.[82] The Department of Justice International Organized Crime Intelligence and Operations Center has worked with Romanian justice officers for over 10 years to successfully arrest and charge Romanian-based organized crime networks that specialize in

[80] European Network and Information Security Agency, *Romania Country Report*, May 2011, European Union at http://www.enisa.europa.eu/act/sr/files/country-reports/Romania.pdf/view.
[81] Safernet, *Safernet - Hotline for a safer Internet*, http://www.safernet.ro/.
[82] Ovidiu Posirca, "FBI Director visits Romania," Business Review at http://business-review.ro/news/fbi-director-visits-romania/12947 (accessed 5 January 2012).

phishing, credit card and ATM thefts, auction fraud, and other forms of cybercrime.[83]

Commonwealth of Independent States (CIS)

The Commonwealth of Independent States (CIS) is a regional organization founded after the breakup of the Soviet Union in 1991, and whose member states are the following former Soviet Republics: Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, and Uzbekistan. In addition, there are two unofficial members of CIS: Turkmenistan and Ukraine. Georgia was a member of CIS since 1994, but ceased its participation in 2009, after the 2008 Georgia-Russia crisis. Cyber-security in CIS countries is discussed as part of information security, and is always included in it, implicitly or explicitly.

An Agreement on Establishment of the Regional Commonwealth in the field of Communications (RCC) was signed by CIS members in 1992. The RCC's mission is to carry out cooperation between the member states in the field of telecommunication and postal communication.[84] Ukraine, Georgia and Turkmenistan are also official members of the RCC.[85] RCC participants determine collaboration around information security and trans-border information exchange between member states.[86] In 1998, the Information Security Commission of the Coordination Council of the CIS member states was established within the RCC. The commission is responsible for developing cooperative proposals on information security matters and for harmonizing national legislation systems accordingly.[87]

In 2011 a report on the main services and tariffs on cybercrime in CIS countries in 2010 was released by Group-IB, a business group, which positions itself as Russia's only company that offers investigation of cybercrimes to businesses.[88] The report discusses cybercrime as a market, and presents its economic analysis from this point of view. Group-IB estimated the financial turnover of the global market for computer crimes to be $7 billion in 2010, of which criminals from CIS countries were estimated to pocket $ 2.5 billion, or roughly one-third. According to

[83] Jay Decenella, "Cyber Crime Involving Romanians Targeted by DOJ, Romanian Police," inAudit at http://inaudit.com/audit/it-audit/cyber-crime-involving-romanians-targeted-by-doj-romanian-police-6897/ (accessed 5 January 2012).
[84]Regional Commonwealth in the field of Communications, *Official website: About*, Commonwealth of Independent States at http://www.en.rcc.org.ru/index.php/rcc/about-rcc (accessed 4 December 2011).
[85] Regional Commonwealth in the field of Communications, *RCC participants*, Commonwealth of Independent States at http://www.en.rcc.org.ru/index.php/rcc/rcc-participants (accessed 4 December 2011).
[86] Regional Commonwealth in the field of Communications, *Strategic lines of activities*, Commonwealth of Independent States at http://www.en.rcc.org.ru/index.php/rcc/strategic-lines-of-activities- (accessed 4 December 2011).
[87] Donos Alexander, *Activities of the Commission on Information Security under Coordinating Council of the CIS Member States on Informatization attached to RCC*, International Telecommunications Union at http://www.itu.int/ITU-D/cyb/events/2008/sofia/docs/donos-RCC-overview-sofia-oct-08.pdf (accessed 13 December 2011).
[88] Group IB, *"Russian" Cybercrime Market in 2010: State and Trends*, 2011, at http://www.group-ib.ru/wp-content/uploads/2011/03/GIB-Issl-rynka_2010.pdf (accessed 4 December 2011). [Document in Russian]

Group-IB, the CIS cybercrime market increased substantially due to weak information security legislation and poor law enforcement in the post-Soviet countries, coupled with a high level of technical education, a common language (Russian), and an unstable economy. The report also presented some prices for different types of cybercrimes on CIS's black market of computer crime services.

The approaches to cyber-security of three CIS-RCC countries – Russia, Belarus and Ukraine – are presented in more detail below.

Russia

Overview

The approach to ensuring cyber-security in Russia is not officially documented or publicly available because the strategy is not fully developed. However, the Russian Ministry of External Affairs proposed a UN convention on International Information Security Provision, which is expected to become the basis for the Russian national cyber-strategy.[89] The main terms of this document are discussed below. Russia's approach is to establish common international rules prior to national strategies, in order to protect the world from international cyber-war.

The International Conference on Cyber Security Attacks held in London in 2011 revealed a public dispute between Russia and other members of the international community over Russia's goals, and whether Russia is ultimately after more state control over the internet.[90] One of the terms in the Russian UN convention draft will allow countries to control and censor the internet inside their boundaries without international intervention.[91] US officials have claimed that "Russia has made cyberspace attack a major factor in its military strategy in order to coerce 'near abroad' nations to align with Russian national interests".[92] The nature of such alleged attacks indicates that the Russian strategic approach for dominance in cyberspace and ensuring its own cyber-security is not through the theft or destruction of Russia's adversaries data but, rather, through the disruption of internal and external communication and information flows.

Russia (and China) often uses the term "informationization", by which it means the intensive exploration and use of information resources for social and economic development. As well, the term "information security" in Russia is a broader notion than in the Anglosphere, emphasizing

[89] Department of Public Information: News and Media Division, *Unregulated Information Highway is Non-Traditional Security Threat with Too Many 'Traffic Accidents', China Tells First Committee, Warning of Security Breaches*. UN General Assembly at http://www.un.org/News/Press/docs/2011/gadis3442.doc.htm (accessed 15 December 2011).
[90] Olga Dmitrieva, "Russia will not close Web," Russian Newspaper at http://www.rg.ru/2011/11/03/shegolev.html (accessed 3 December 2011). [Document in Russian]
[91] "Convention of Russian Federation against Cyber Wars," Interfax News Agency at http://www.interfax.ru/politics/txt.asp?id=209093 (accessed 4 December 2011). [Document in Russian]
[92] Richard G. Zoller, *Russian Cyberspace Strategy and a Proposed United Stated Response*, January 2010, US Government at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA522027.

national security over personal computer security.[93] The Information Security Doctrine of the Russian Federation, ratified in 2000, includes some points on national cyber-strategy.[94] The second part of the Doctrine discusses types of threats to information security. These were also incorporated into the Russian Criminal Code. The fourth component of this doctrine includes the protection of information resources from unauthorized access, and the security of information and telecommunications systems that are already deployed and that are being established on the territory of Russia.

Role of the Public Sector – Policy

There is no special public department that deals particularly with cyber-security and monitors the activities on cyberspace in Russia. Activities in this area, as are all governmental activities, appear to be centralized in the president and prime minister's offices. However, according to the Russian private sector, Russia is contemplating the establishment of such a department as it develops its strategy.[95]

The State Duma Committee on Information Policy, IT and Communication regulates media organizations, media relations with citizens, communications, the use of radio spectrum, and the use of public ICT networks, including the internet. However, due to budget cuts the Russian parliament decided to eliminate this committee as of 2012. Its responsibilities will be assigned to the Committee of Culture.[96]

Russia distinguishes between external and internal threats. According to the doctrine mentioned above, external threats include: the activities of foreign countries directed against Russian information interests, the intensification of international competition in information technology, the activities of international terrorist organizations, and the development of information espionage and warfare.[97]

The Institute of World Economy and International Relations of the Russian Academy of Sciences, which is not formally part of the Russian government, produced a report on "Cyber-wars and International Security".[98] The report addresses such issues as transactions in cyberspace

[93] John Markoff, "At Internet Conference, Signs of Agreement Appear Between U.S. and Russia," *New York Times*, 15 April 2010, Science section at http://www.nytimes.com/2010/04/16/science/16cyber.html.
[94] "The Information Security Doctrine of the Russian Federation," deHack at http://dehack.ru/zak_akt/npa_prezidentarf/doktrina_ib/?all (accessed 3 December 2011). [Document in Russian]
[95] Oleg Sincha, "Russian secret services should prepare for cyber-war," Digit.ru at http://digit.ru/state/20111212/387789149.html (accessed 13 December 2011). [Document in Russian]
[96] Natalia Lavrentieva, "State Duma licvidated the Committee on IT and Communications," CNews at http://www.cnews.ru/news/top/index.shtml?2011/12/20/469659 (accessed on 20 December 2011). [Document in Russian]
[97] "The Information Security Doctrine of the Russian Federation," Russian Newspaper at http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm (accessed 3 December 2011). [Document in Russian]
[98] "Convention of Russian Federation against Cyber Wars," Interfax News Agency at http://www.interfax.ru/politics/txt.asp?id=209093 (accessed 4 December 2011). [Document in Russian]

as an integral component of information operations, the main provisions of the American doctrine on "cyber-wars", the development of the organizational structure of US warfare in cyberspace, and the conceptual basis of "information warfare" in China. This research indicates where Russian interests are focused and will help Russian officials in the development of their national cyber-strategy.

Role of the Public Sector – Law

Several significant federal statutes relating to cybercrime were passed in Russia in the 1990s. The Act About Information, Informationization and Information Protection was passed in 1995, The Act About Legal Protection of Software for Computers and Databases was passed in 1992, and The Act About Copyright and Related Rights, The Act About State Secrets and The Act About Communication were passed in 1993.[99]

Article 28 of the Russian Criminal Code addresses Computer Information Crimes and was amended in 2011. The Article defines criminal cyber-activity and has the following three clauses: Clause 272 – Illegal Access to Computer Information; Clause 273 – Creation, Use and Distribution of Malware Software on Computers; and Clause 274 – Violation of Rules of Usage of Computers, Computer Systems or Computer Networks.

Clause 272 deals with invasion of privacy and identity theft. Clause 273 deals with malware, and Clause 274 refers to other Russian legislation that protects computer information.[100] The same amendment, however, deleted an earlier clause that criminalized "causing damage to computers and computer networks", making the prosecution of organizers of denial of service attacks harder.[101]

Russia has not signed the Budapest Convention on Cybercrime yet, because it claims that accepting the convention would grant foreign law enforcement agencies the authority to intercept Russian internet traffic.[102] Ratification would also obligate Russia to recognize as criminal acts such activities as the acquisition and possession of devices and computer programs designed or adapted for the commission of a crime (i.e., malware), as well as the acquisition and possession of computer passwords, access codes or other similar data that can be used to access a computer system or its part. As described above, Russian criminal law criminalizes the creation, use and dissemination of malicious software, but not its possession. A similar change would be required

[99] Victor Karpov, *Criminal liability for the crimes in the field of computer information*, 2002, Krasnoyarsk State University at http://mirt-d.ru/ugolov-komp.html (accessed 3 December 2011). [Document in Russian]
[100] "Legislation in the field of information security," L-Soft Company at http://www.lcnsoft.ru/index.php?option=com_content&view=article&id=27&Itemid=37&lang=ru (accessed 4 December 2011). [Document in Russian]
[101] "Russia updated the law on cybercrimes," Segodnya.ua at http://www.segodnya.ua/news/14315998.html (accessed 4 December 2011). [Document in Russian]
[102] Pavel Domkin, "Criminal liability for committing computer (cyber) crimes in accordance with international law," Domkins and Partners at http://www.advodom.ru/practice/cybercrime-2.php (accessed 2 January 2012). [Document in Russian]

in the Russian criminal offence of child pornography (Article 242.1) which currently only criminalizes the creation, use, distribution and possession with intention to distribute of child pornography.[103]

Role of the Private Sector – For-Profit

One of the objectives of the Russian information security strategy is to bring all communication networks and computer systems across Russia and inside the Russian Ministry of Internal Affairs to one common standard. The Russian government handed over the administration of this project to the Science and Technology Center of European-Asian Association of Security Products and Services Providers.[104] This association was established in 1997 to shape and develop the market of security products and services in Russia. Nowadays it is a multi-disciplinary business entity that has the appropriate licenses and certificates from the Russian Federal Security Service, Russia's Federal Service for Technology and Export Control, the Russian Emergencies Ministry and the Ministry of Transport. The project was awarded in 2011 to the Kaspersky Lab.[105]

Cooperation with other jurisdictions

As mentioned above, Russia drafted a UN Convention in 2011 on international information security. The draft aims to reduce the possibility of international cyber-war, but there seem to be a common opinion among Russian and American analysts that the real purpose of this document is to protect Russia from international retaliation. The draft supports the idea of "national internets", and stresses that the security problems on the internet should be solved within the country that has the problem without intervention from other countries. Critics argue that the provisions offered by the Russian Ministry of External Affairs will not affect national security but rather limit the freedoms of law-abiding citizens.[106] Countries that have already invested in military cyber-divisions will probably resist signing the convention.

At the 2011 London Conference Russia suggested establishing a "cyberspace code of conduct", which was essentially its draft UN Convention. Russian officials acknowledge that many countries would not want to sign their draft, but believe that the development of a common international code is important.[107]

---

[103] "Section 242.1. Manufacturing and sales of materials or objects with pornographic images of minors," The Criminal Code of Russian Federation at http://www.ukru.ru/code/09/242.1/index.htm (accessed 5 December 2011). [Document in Russian]

[104] The Science and Technology Center of European-Asian Association of Security Products and Services Providers, *About the organization*, at http://www.evraas.ru/index.php?option=com_content&view=article&id=18&Itemid=5.

[105] "'Kaspersky Lab' will provide cyber-security for Ministry of Interior Affairs of Russian Federation," Kaspersky Lab at http://www.kaspersky.ru/news?id=207733601 (accessed 13 December 2011). [Document in Russian]

[106] Savva Kozlovsky, "Russian Ministry of Interior Affairs will deal with cyber-security," Mnenia.ru at http://mnenia.ru/rubric/tech/mid-rossii-zaymetsya-kiberbezopasnostyu/ (accessed 14 December 2011). [Document in Russian]

[107] Olga Dmitrieva, "Russia will not close Web," Russian Newspaper at http://www.rg.ru/2011/11/03/shegolev.html (accessed 3 December 2011). [Document in Russian]

Furthermore, in 2011 the US and Russia signed a pact on cooperation in information security, which includes the agreement to exchange information about imminent cyber-offenses, and information exchange between the computer emergency response teams of both countries.[108] Both Russia and the US are concerned ostensibly about state-initiated cyber-attacks, since these are difficult to formally link to specific governments. The Russian approach advocates the need for common international legislation or a common code of conduct in cyberspace, while maintaining national independence of action. The US, on the other hand, considers such international regulation an unnecessary restraint, and advocates for improved cooperation between countries and international law enforcement groups.[109] Of course, Russia has been accused of cyber-attacks against Estonia in 2007 and Georgia in 2008. Both attacks used bot-nets and the Russian government denied involvement.

Belarus

Overview

The Belarus government sees the main danger not in cyber-attacks on its information systems but in Belarus citizens' social and political activity outside of governmental control. A presidential decree, "On Measures of Improvement of the National Segment of the Internet" was introduced in 2010. According to this decree, owners of internet cafes are required to identify individual customers and service providers have to store information about all the webpages that are visited by users.[110]

Belarus also published in 2010 its information security strategy, titled "Concept of the National Security of Republic of Belarus".[111] Among the security priorities are: the development and introduction of modern methods and means for protecting information technologies that are used primarily in weapon and troop control systems; environmentally hazardous and economically important infrastructure; state control over the design, creation, development and the use of the means for information security; and, providing legal and organizational conditions for the prevention, detection, and combat of crime in the information area.[112]

---

[108] Valeriy Ledovskoi, "Russia and the U.S. signed a pact in the field of computer security," Anti-Malware News at http://www.anti-malware.ru/news/2011-07-16/4312 (accessed 5 December 2011). [Document in Russian]
[109] John Markoff and Andrew E. Kramer, "U.S. and Russia Differ on a Treaty for Cyberspace," *New York Times*, 27 June 2009, World Section at http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all.
[110] The President of the Republic of Belarus. *Presidential Decree of 1 February 2010*, Belarus Government at http://president.gov.by/data/press83054.doc. [Document in Russian]
[111] State Committee on Science and Technology of the Republic of Belarus, *The Concept of National Security of the Republic of Belarus*, Belarus Government at http://gknt.org.by/rus/bulletin/20100910/20100910/ (accessed 17 February 2012). [Document in Russian, for English translation of this document see http://www.canada.belembassy.org/eng/copy_legislation_2618/concept_of_the_national_security_of_the_republic_of_belarus/]
[112] From A.N Kurbatsky (ed), *Materials on XVI Theoretical and Practical Conference* (Minsk, Belarus, 2011), 24.

Role of the Public Sector – Policy

The state-owned Beltelecom monopoly is the sole provider of telephone and internet connectivity, although about 30 national ISPs connect through Beltelecom. The only reported independent internet link is via the government's academic and research network, BasNet. Strict government controls are enforced on all telecommunications technologies; for example, transceiver satellite antennas and IP telephony are prohibited. Beltelecom has been accused of "persecution by permit" and of requiring a demonstration of political loyalty to access its service.[113]

The State Center for Information Security (GCBI), in charge of domestic signals intelligence, controls the ".by" top level domain and, thus, manages both the national domain name service and website access in general. Formerly part of the Belarusian KGB, the GCBI reports directly to President Lukashenko. Department "K" (for Кибер or Cyber) within the Ministry of Interior has the lead in pursuing cybercrime. A common media offence in Belarus is defaming the "honour and dignity" of state officials.

Belarus has developed a four-year State Scientific and Technical Program, "Development of Methods and Tools for Integrated Information Security" (also known as "Information Security-2") for 2011-2015, which is primarily focused on the implementation of the Concept of the National Security of Republic of Belarus.

Role of the Public Sector – Law

Belarus passed the Law About Informationization in 1995, that was amended in 2006; it defines the concept of informationization and its main principles.[114] Article 4 describes national policy in the informationization area. This article prescribes that the government has the following responsibilities: organize the formation and use of information resources of the republic; ensure public support for informationization; take action to improve the quality of documented information and information services; stimulate the creation of modern information technology, information systems and networks; support the development of communication systems; create the conditions for openness, accessibility and security of information resources; regulate relations in the area of informationization through the investment, tax and budget policy; and, establish public authorities on matters of informationization. Article 5 describes the "Protection of Information Resources and the Rights of Informationization Parties" and presents the basic objectives of information protection (to prevent information leaks or distortion, preserve documented information, protect the rights of the informationization parties, etc.).

[113] This and the next paragraph contain extracts from Kenneth Geers, *Strategic Cyber Security* (Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2011), 72 -73.
[114] Republic of Belarus, *The Law About Informationization, 6 September 1995, with amendments of 20 June* 2006, Commonwealth of Independent States at http://tammby.ru/belarus-zakon/zakon_3850-1995.htm (accessed 27 December 2011). [Document in Russian]

In 2008 Belarus passed the Law About Information, Informationization and Information Protection,[115] which deals with information security more directly. Violations of this law are either administrative, as per the Code of Administrative Offences (Chapter 22, "Administrative Violations in the Field of Communication and Information")[116] or criminal, as per the Criminal Code of the Republic of Belarus (Chapter 31, "Crimes Against Information Security").[117]

Articles 349-355 of Chapter 31 of the Criminal Code define the following types of computer crimes: unauthorized access to computer information; modification of computer information; cyber sabotage; illegal possession of computer information; creation or distribution of special means for unauthorized access to computer system or network; development, use or distribution of malicious software; and, violation of the rules of operation of computer systems or networks.

In 2012 new amendments to the Code of Administrative Offences should enter into force in Belarus. According to these amendments, Belarusian citizens will not be able to visit foreign websites, i.e. websites that have their servers located outside the Belarus national borders. Penalties of up to 1 million Belarusian Rubles (equivalent to $120) will be imposed. The law will apply not only to private individuals but also to businesses.[118]

Role of the Private Sector – For-Profit

Under the authoritarian government of Belarus there is no genuine private sector to speak of. The Belarus company VirusBlockAda is the only developer of antivirus software in the Republic of Belarus. Their product is the antivirus VBA-32 for personal computers running Microsoft Windows. They are endorsed by the Belarus government and state, with the primary strategic objective to develop and support a national program on protection against the impact of malware.[119] Another Belarus company, S-Bel Terra, develops network security products. It was founded by the Russian network security company S-Terra CSP, the first technological partner of Cisco Systems in Russia.

Role of the Private Sector – Not-For Profit

The not-for profit sector is non-existent in Belarus.

---

[115] Republic of Belarus, *On information, informationization and information protection*, Valery Levaneuski Personal Site at http://pravo.levonevsky.org/bazaby09/sbor00/text00878.htm (accessed 3 January 2012). [Document in Russian]

[116] Republic of Belarus, "The Code of Administrative Offences of Belarus, Chapter 22," City of Grodno at http://uvd.grodno.by/index.php?option=com_content&view=article&id=1536%3Aglava-22&catid=34&Itemid=188 (accessed 3 January 2012). [Document in Russian]

[117] Republic of Belarus, "Crimes against information security," Legal Forum of the Republic of Belarus at http://www.yurist.by/glava-31-prestupleniya-protiv-informatsionnoi-bezopasnosti (accessed 3 January 2012). [Document in Russian]

[118] Federico Guerrini, "Foreign websites are banned," *La Stampa*, 4 January 2011 at http://www.lastampa.it/_web/cmstp/tmplrubriche/tecnologia/grubrica.asp?ID_blog=30&ID_articolo=9939. [Document in Italian]

[119] VirusBlockAda, *About the Company*, at http://www.anti-virus.by/about/vba/.

Cooperation with other jurisdictions

There is active cooperation between Belarusian and Russian intelligence agencies in cyberspace, as specified in the Agreement on Cooperation of the Commonwealth of Independent States (CIS) in Combating Cybercrime, signed in 2000.[120]

Although there is generally disagreement between the EU and Belarus,[121] in 2011 the European Union and the Council of Europe launched a project in cooperation with several "Eastern Partnership" countries (Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine) against cybercrime. "The specific project purpose is to strengthen the capacities of criminal justice authorities of the Eastern Partnership countries to cooperate effectively against cybercrime in line with European and international instruments and practices".[122]

Ukraine

Overview

There is no official statistical data about cybercrime activity in Ukraine. According to external sources, crimes committed using information technology are in the top five most common economic crimes in Ukraine. More than 25% of organizations in Ukraine do not have adequate cybercrime incident response mechanisms.[123]

Ukraine underwent a massive cyber-attack late in 2011 by a group known as Kosovo Hackers Security (KHS). The group hacked more than 600 websites in Ukraine, including the official website of the Ukraine Police, Gazeta.ua (Ukraine's largest news portal) and many more high profile websites.[124] The organization claimed to have patriotic and political reasons for this attack. Ukrainian officials did not comment on this event and a strategy to respond to similar events has not yet been formulated or made public.

Role of the Public Sector – Policy

The Security Service of Ukraine (Sluzhba Bezpeky Ukrayiny – SBU) is the main government security agency responsible for the development of national cyber-securitystrategy

[120] Kenneth Geers, *Strategic Cyber Security* (Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2011), 79.
[121] European Commission, *Restrictive measures*, January 2012, European Union at http://eeas.europa.eu/cfsp/sanctions/docs/measures_en.pdf.
[122] Economic Crime Division, *Eastern Partnership – Cooperation against Cybercrime*, Council of Europe at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_project_eap/May11_Tallinn_Launching_event/2523%20Act-0%20launch%20outline.pdf (accessed 3 February 2012).
[123] "Ukraine Global Economic Crime Survey: Cybercrime in the spotlight," December 2011, PriceWaterhouseCoopers at http://www.pwc.com/ua/en/press-room/assets/GECS_Ukraine_en.pdf (accessed 4 January 2012).
[124] Vogh Reporter, "Ukraine Under Massive Cyber Attack by Kosovo Hackers Security," Voice of Grey Hat at http://www.voiceofgreyhat.com/2011/12/ukraine-under-massive-cyber-attack-by.html (accessed 4 January 2012).

in Ukraine, subject to the approval of the president. The Doctrine on Information Security (2009) highlights the main areas of public policy related to information security in Ukraine: foreign policy, national security, military, internal affairs, economy, social and humanitarian affairs, scientific-technological development, and ecology.[125]

Role of the Public Sector – Law

Ukraine has a number of national laws covering issues of cyber-security, such as On Main Principles of Information Society Development In Ukraine; On State Service of Special Communication and Information Protection of Ukraine; On Information Security in Information and Telecommunication Systems; and On The Fundamentals Of National Security Of Ukraine.[126]

The first law in Ukraine aimed at regulating computer crime was Article 198-1 of the Criminal Code of Ukraine (1992). The article provided a broad coverage of the different forms of computer crime and methods to commit it, and, until recently, was the only legal instrument dealing with cybercrime. In 2001, a new version of the Criminal Code was adopted and entered into force with an expanded chapter on cybercrime. Chapter XVI – Crimes in the Use of Computers, Computer Systems and Computer Networks consists of Articles 361, 362, 363.[127] Computer crime is defined as a socially dangerous act in which computer information is the subject of a criminal assault.[128] Few other terms are defined however, and the National Institute for Strategic Studies suggested some amendments to the current legislation, including adding the definitions for the following terms: cyber-space, cyber infrastructure, critical cyber infrastructure, cyber-security, cyber-attack, cybercrime, and cyber-terrorism.[129]

Role of the Private Sector – For-Profit

There is a lack of IT market segmentation in Ukraine. The information security companies that are currently present in Ukraine are either well-known branches of international companies or Russian companies. For example, the Centre for Information Security LLC is a Ukrainian company specializing in information technology and information security. The company has a free online portal about laws and news in information security;[130] the portal is in

[125] President of Ukraine, "The Doctrine on Information Security," Ukrainian Government at http://www.president.gov.ua/documents/9570.html (accessed 3 December 2011). [Document in Ukrainian]
[126] Verkhovna Rada of Ukraine, "The Law of Ukraine On Information Security in Information and Telecommunication systems," Ukrainian Government at http://zakon2.rada.gov.ua/rada/show/80/94-%D0%B2%D1%80/conv (accessed 2 December 2011). [Document in Ukrainian]
[127] "Criminal Code of Ukraine, Chapter XVI: Crimes in the Use of Computers, Computer Systems and Computer Networks," Computer Crime Research Center at http://www.crime-research.ru/library/npkrus.htm (accessed 4 December 2011). [Document in Russian]
[128] Mikhail Dutov, "Liability for computer crimes according the new version of the Criminal Code of Ukraine," Computer Crime Research Center at http://www.crime-research.ru/library/dutov.htm (accessed 4 December 2011). [Document in Russian]
[129] The National Institute for Strategic Studies, "The problems of the current national legal framework for combating cybercrime: Main Directions for reform," Ukrainian Government at http://www.niss.gov.ua/articles/454/ (accessed 17 December 2011). [Document in Ukrainian]
[130] Ukrainian Information Security Center, *Information Security Center*, at http://www.bezpeka.com.

the top-ten most visited websites in Russian about information security. However, for most IT companies information security products are not their main line of business, and they are not integrated into the Ukrainian strategy.

Role of the Private Sector – Not-For Profit

The Ukrainian Information Security Group (UISG) plays an important role in developing the information security community in Ukraine.[131] The Group works in co-operation with the Kiev branch of ISACA, and regularly holds conferences in Ukraine on current cyber and information security issues.[132]

Cooperation with other jurisdictions

Ukraine ratified the Budapest Convention in 2006. Since the country's independence from the Soviet Union, Ukraine has been cooperating with NATO on several issues including cyber-security, aspiring to become a member of the alliance.[133] The first meetings of the Ukraine-NATO Working Subgroup on Cyber-Security took place in 2010. Within the framework of this group Ukraine receives expert support from the NATO concerning drafting the National Strategy on fighting cyber-challenges, developing cyber-defense infrastructure and a response system to cyber-threats in Ukraine.[134]

Additionally, Ukraine collaborates with the CIS. In 2011, it hosted the 17th Security of Information in Telecommunications Networks conference. The conference was attended by experts from Azerbaijan, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Russia and Uzbekistan. Legal, scientific, technical and economic aspects of information security were discussed. Ukraine presented the main concepts of the draft of the new Ukrainian Law On Cyber Security, the document that should become the basis for the national cyber-security strategy that Ukraine is developing in close cooperation with NATO.[135]

Ukraine takes part in all NATO and CIS initiatives, yet it is not an official member of either alliance, so it does not get the benefits of a member state. Ukraine also wants to join the EU, and will have to satisfy European standards on cyber-security, among other requirements for joining the union.

---

[131] "The Ukrainian Information Security Group," LinkedIn at http://www.linkedin.com/groups?home=&gid=1220117 (accessed 20 December 2011).
[132] ISACA, *About the organization*, at http://www.isaca.org/about-isaca/Pages/default.aspx.
[133] Dirk Brenhelmann, "20 Years of cooperation between NATO and Ukraine," North Atlantic Treaty Organization at http://www.nato.int/nato_static/assets/pdf/pdf_2011_nidc/20111012_110719u.pdf (accessed 10 December 2011). [Document in Ukrainian]
[134] Embassy of Ukraine in the UK and Northern Ireland, "Ukraine-NATO Relations," Ukrainian Government at http://www.mfa.gov.ua/uk/en/30717.htm (accessed 14 December 2011).
[135] "A Conference on Cyber-security in the CIS is happening in Kiev," UNIAN News Agency at http://www.unian.net/rus/news/news-436329.html (accessed 15 December 2011). [Document in Russian]

Baltic Region

All the Baltic countries are members of the EU, and, hence, have European Network and Information Security Agency (ENISA) assistance and support in developing information security strategies and improving information networks.[136]

The Baltic countries hold regular summits in which cyber-security and related issues are sometimes discussed. The Baltic countries are also members of Nordic-Baltic cooperation, or NB8, together with the Nordic countries Denmark, Sweden, Finland, Norway and Iceland. In 2010 NB8 produced the Co-operation Report (subsequently named NB8 Wise Men Report) with recommendations on "civil security, including cyber security".[137] The authors of the report suggest enhancing cooperation concerning cyber-security, establishing a multilateral security agreement, and implementing a "capacity building of Computer Emergency Response Teams (CERT) in relevant NB8 countries".[138]

Estonia

Overview

The responsible authority for the development of the national cyber-security strategy in Estonia is the Cyber-Security Strategy Committee of the Ministry of Defence. In 2008 it released the official Cyber-Security Strategy, which presented the position of Estonia on cyber-attacks, threats in cyberspace, the national and international legal framework to fight cybercrime, and goals on enhancing cyber-security in Estonia.[139]

Role of the Public Sector – Policy

The national strategy for cyber-security was introduced just after the cyber-attacks on Estonia in 2008. Estonian cyber-security action plans are integrated in the national security planning, and are the responsibility of the Ministry of Defence (the Estonian President did distinguish between cyber-attacks and cyber-war).[140] The Cyber Security Strategy Committee in the Ministry of Defence cooperates with the Ministry of Education and Research, the Ministry of Justice, the Ministry of Economic Affairs and Communications, the Ministry of Internal Affairs, and the Ministry of Foreign Affairs.

The strategy identified the following policy priorities: application of a graduated system of security measures in Estonia; development of Estonia's expertise in, and high awareness of, information security to the highest standard of excellence; development of an appropriate

[136] European Network and Information Security Agency, *Homepage*, at http://www.enisa.europa.eu.
[137] Ministry for Foreign Affairs, *NB8 Wise Men Report*, August 2010, Icelandic Government at http://www.utanrikisraduneyti.is/media/Skyrslur/NB8-Wise-Men-Report.pdf.
[138] Ministry for Foreign Affairs, *NB8 Wise Men Report*, August 2010, Icelandic Government at http://www.utanrikisraduneyti.is/media/Skyrslur/NB8-Wise-Men-Report.pdf.
[139] Ministry of Defence, *Cyber Security Strategy*, 2008, Estonia Government http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf.
[140] "Estonian President says that cyber attacks is not a cyberwar," Russian Community Portal Estonia at http://baltija.eu/news/read/21846 (accessed 5 January 2012). [Document in Russian]

regulatory and legal framework to support the secure and seamless operability of information systems; and, promoting international co-operation aimed at strengthening global cyber-security.[141]

Supervision over the implementation of freedom of information legislation in Estonia is carried out by the Data Protection Authority, which annually reports to the Estonian Legislature on compliance with the Public Information Act. Any person who has been denied access to requested information may file a complaint with the Data Protection Authority or with an administrative court.[142]

The Estonian Information Society Strategy 2013 was drafted by the Ministry of Economic Affairs and Communications in 2007, and the Implementation Plan 2010-2011 of this strategy was approved in 2010. The priorities of the plan were the development of Estonia's next generation broadband network, electronic businesses environment, public services, the large-scale uptake of e-ID, and increasing the interoperability of state information systems.[143]

Role of the Public Sector – Law

The Estonian legal framework for cyber-security is yet to be updated. The right to access information held by public authorities is declared as a constitutional right of citizens and defined under Article 44 of Estonian Constitution. The basic legal act regulating access to publicly important information is the Public Information Act, 2001. Other relevant laws are the Data Protection Act, Archives Act, State Secrets Act and Environmental Register Act.[144] There is no clear legal basis for regulating the transmission of data by internet service providers or for the termination of internet connections in cases where computers have been compromised.

There are six Articles related to cybercrime and security in the Estonian Penal Code – 206, 207, 208, 213, 217, and 284 – that set punishment for the following crimes: computer sabotage; damaging of a connection to a computer network; spreading of computer viruses; computer-related fraud; unlawful use of a computer, computer system or computer network; handing over protection codes.[145]

---

[141] Ministry of Defence, *Cyber Security Strategy*, 2008, Estonia Government http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

[142] Office for Democratic Institutions and Human Rights, "Access to Information and Data Protection: Estonia," Organization for Security and Co-operation in Europe at http://legislationline.org/topics/country/33/topic/3 (accessed 20 January 2012).

[143] European Network and Information Security Agency, *Estonia Country Report*, May 2011, European Union at http://www.enisa.europa.eu/act/sr/files/country-reports/Estonia.pdf.

[144] Office for Democratic Institutions and Human Rights, "Access to Information and Data Protection: Estonia," Organization for Security and Co-operation in Europe at http://legislationline.org/topics/country/33/topic/3 (accessed 20 January 2012).

[145] European Network and Information Security Agency, *Estonia Country Report*, May 2011, European Union at http://www.enisa.europa.eu/act/sr/files/country-reports/Estonia.pdf.

Role of the Private Sector – For-Profit

Several private sector companies play a role within Estonia's strategy. AS Sertifitseerimiskeskus is Estonia's certification authority, providing certificates for authentication and digital signing of Estonian ID Cards.[146] The core function of AS Sertifitseerimiskeskus is to ensure the reliability and integrity of the electronic infrastructure behind the Estonian ID Card project. It is a joint venture of the two leading Estonian banks, Hansapank and SEB, together with two telecom companies, Elion and EMT. The company is currently offering its services, including involvement in R&D projects, across the Baltics.

Real Systems Ltd. is a professional information systems and software design and development company based in Estonia with a subsidiary in Moldova. It has clients in fifteen countries across the CIS. The company develops nation-wide and web information systems for the public sector, and also offers solutions for cyber investigations.[147]

Role of the Private Sector – Not-For Profit

In 2009 Estonian IT professionals and the government started a government-to-citizen project, Arvutikaitse[148], to raise awareness about security issues on the internet. IT professionals have also volunteered for the National Cyber Defence League – Küberkaitseliit (KKL), established in 2009, that focuses on the defence of telecommunication infrastructure from cyber-attacks in Estonia. Other not-for profit organizations also attempt to raise awareness. Among them are the Look at the World Foundation (running an IT security portal), and the ETL (Estonian Consumers Union – Eesti Tarbijakaitse Liit), a consumer organization that aims to protect and educate consumers.[149]

Cooperation with other jurisdictions

Estonia is a member of NATO – its cyber-security strategy was created under NATO's umbrella and influenced by NATO's Cyber Defence Policy. According to Estonia's 2008 strategy, it will assume a leading role in introducing cyber security-related initiatives to international organisations and through bilateral co-operation. The Council of Europe convention on combating cybercrime and the work of EU institutions on defending critical information infrastructure are an important part of the strategy, as are the cyber-security and IT initiatives of the United Nations.

NATO's Cooperative Cyber Defence Centre of Excellence (established 2008) is located in Tallinn, Estonia. The purpose of this organization is "to enhance NATO's cyber defence capability". Besides Estonia, other members of the centre are Latvia, Lithuania, Germany,

[146] AS Sertifitseerimiskeskus, *About SK*, at http://www.sk.ee/en/about.
[147] Real Systems, *Official webpage*, at http://www.rs.ee/eng/index2.html.
[148] Computer Protection, *Information Security Signpost*, at http://www.arvutikaitse.ee. [Document in Estonian]
[149] Estonian Consumer Union, *Estonian Consumer Union's website*, at http://www.tarbijakaitse.ee. [Document in Estonian]

Hungary, Italy, Poland, Slovakia, Spain, and the US. In 2011 NATO experts started training specialists in Estonia at the centre, in order to be able to repel internet cyber-attacks.[150]

Lithuania

Overview

The Lithuanian national cyber-security strategy has been developed but not yet deployed.[151] Delfi, a major internet portal in the Baltic States, reported in 2012, that "politicians endorsed the National Cyber Security Development Program in June 2011, but after the government hastily cut state institutions' budgets at the end of 2011, no funds for the implementation of this document have been allocated yet".[152] The government has established an Action Plan but it is focused on the improvement of electronic services and ICT.[153] Lithuania's network infrastructure is considered poor, and the country's bandwidth may be insufficient to cope with a large number of security attacks.[154]

Role of the Public Sector – Policy

The Ministry of Transport and Communications is responsible for the development of cyber-security initiatives and national strategy. The Ministry of the Interior creates state policy in the field of IT security. It prepares and approves draft laws on IT security; draft orders of the Minister of the Interior; drafts resolutions of the Government and other legal acts on IT security; controls the implementation of state policy in the field of IT security; organizes the performance of functions of the Security Accreditation Authority; coordinates IT projects allocated within the competence of the Ministry; supervises the implementation of state policy in the field of personal identification in cyberspace; and, coordinates IT security in state institutions and establishments.[155]

Role of the Public Sector – Law

While Lithuania has drafted legislation on network and information security, none has been passed as of 2011. The Law on Electronic Communications has existed since 2004 (last amended in 2009). It regulates electronic communications services and networks with their

[150] Tatiana Karpenko, "NATO helps Estonia to fight cybercriminals," Deutsche Welle at http://www.dw-world.de/dw/article/0,,15153234,00.html (accessed 14 December 2011). [Document in Ukrainian]
[151] European Network and Information Security Agency, *Lithuania Country Report*, May 2011, European Union at http://www.enisa.europa.eu/act/sr/files/country-reports/Lithuania.pdf.
[152] "Lithuanian experts concerned about lack of funding for cyber security," Techpost Media at http://techpostmedia.com/content/lithuanian-experts-concerned-about-lack-funding-cyber-security (accessed 4 February 2012).
[153] European Network and Information Security Agency, *Lithuania Country Report*, May 2011, European Union at http://www.enisa.europa.eu/act/sr/files/country-reports/Lithuania.pdf.
[154] European Network and Information Security Agency, *Lithuania Country Report*, May 2011, European Union at http://www.enisa.europa.eu/act/sr/files/country-reports/Lithuania.pdf.
[155] Ministry of the Interior, *Homepage*, Lithuanian Government at http://www.vrm.lt/index.php?id=124&lang=2.

associated facilities and services, the use of electronic communications resources as well as radio and terminal equipment, and electromagnetic compatibility. In 2006 the Law on Information Society Services was adopted. It describes and establishes legal grounds for the regulation of information services. Lithuania has also had personal data protection legislation since 1996 (continuously amended, most recently in 2011).

Role of the Private Sector – For-Profit

There is no formal role for the for-profit sector in Lithuania's developing strategy.

Role of the Private Sector – Not-For Profit

The role of the not-for profit sector is minor. A Public-Private Partnership (PPP) with the purpose of increasing network and information security awareness between the general internet users, SMEs and Lithuanian governmental institutions exists.[156]

Cooperation with other jurisdictions

Lithuania is the coordinator of NB8 in 2012. The country is also an active participant in the Estonian-based centre mentioned above, and in the European contact network of spam authorities.[157]

Latvia

Overview

Latvia is another Baltic country with a cyber-security strategy that has yet to be approved by its parliament. However, as discussed below, it does have relatively well-developed legislation.

Role of the Public Sector – Policy

The Ministry of Transport is the only institution responsible for issues related to resilience and policy development. The National Security Strategy, which includes a section on Information Technology risk prevention, and defines how to provide IT security and how to improve the existing mechanisms, has yet to be approved by the Latvian parliament, as mentioned above.[158]

Role of the Public Sector – Law

[156] Lithuanian Communications Regulatory Agency, *Information portal E-Saugumas*, Lithuanian Government at http://www.esaugumas.lt. [Document in Lithuanian]

[157] Jos Dumortier and Geert Somers. *Study on activities undertaken to address threats that undermine confidence in the Information Society, such as spam, spyware and malicious software SMART 2008/ 0013*, April 2009, European Commission at http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf.

[158] European Network and Information Security Agency, *Latvia Country Report*, May 2011, European Union at http://www.enisa.europa.eu/act/sr/files/country-reports/Latvia.pdf.

New legislation, the Law on Information Technologies Security came into force in 2011. The law establishes an IT Security Incident Response Institution (the national computer emergency response team). It also defines the key requirements for organizations to guarantee the security for the essential electronic services, and determines the behaviours in cases of information technology security incidents.

In 2004, the Electronic Communications Law was introduced, which regulates the provision of electronic communications services according to the EU regulatory framework for electronic communications. The State Information Systems Law (last amended in 2008) establishes Operating Principles for State Information Systems, aiming to ensure the availability and quality of the informative services provided by state and local government institutions.

Four sections in the Penal Code are related to cybercrime and security: Section 241, Arbitrarily Accessing Automated Data Processing Systems; Section 243, Interference in the Operation of Automated Data Processing Systems and Unlawful Actions with the Information included in Such Systems; Section 244, Unlawful Operations with Automated Data Processing System Resource Influencing Devices; and, Section 245, Violation of Safety Provisions Regarding Information Systems.[159]

Role of the Private Sector – For-Profit

The role of the for-profit sector is not well developed within Latvia's strategy.

Role of the Private Sector – Not-For Profit

The Latvian Electrical Engineering and Electronics Industry Association (LetERA) is an independent, voluntary and non-governmental public organization that unites companies, research and educational institutions registered and operating in Latvia, whose activities are related to Industry of Electronics and Electrical Engineering, Information and Communications Technology. It was established to search for solutions of different problems common to several sectors of the ITTE branch. The organization supports cooperation with other branch associations in Latvia and related organizations in EU.

The Latvian Information and Communications Technology Association (LIKTA) is a professional association, founded in 1998, that regroups over 80 important ICTE product and service providers and educational institutions, as well as about 100 individual professional members of the ICTE industry sector in Latvia, namely in computer hardware and software, electronics, and telecommunications infrastructure and service providers.[160] Similarly, the Latvian Internet Association (LIA) was established in 2000. LIA represents more than 90% of Latvian internet service providers and other domestic and foreign enterprises dealing with

[159] European Network and Information Security Agency, *Latvia Country Report*, May 2011, European Union at http://www.enisa.europa.eu/act/sr/files/country-reports/Latvia.pdf.
[160] The Latvian Information And Communications Technology Association, *Homepage* at http://www.likta.lv/en/Pages/home.aspx.

different internet services.[161] Both industry associations attempt to influence government policy but do not have a formal role within the Latvian strategy.

Cooperation with other jurisdictions

Similar to the other Baltic Countries, Latvia is a participant in the Cooperative Cyber Defence Centre of Excellence together with the other sponsoring nations.

China

Overview

China is often perceived as tolerating, and even encouraging, cyber-espionage against foreign states and businesses. At the same time, it suffers a large degree of retail-level fraud and other forms of cybercrime against domestic businesses and individuals. While China possesses the technological sophistication to launch cyber-attacks in other jurisdictions, its domestic territory remains highly susceptible to cybercrime. A Chinese government survey (2003) found that almost 90% of Chinese PCs connected to the internet were infected with malware.[162] According to some sources China is second only to the US as a target of cybercrime, with 23% of all attacks aimed at China, and 24% at the US. The US, on the other hand, is the source of 50% of attacks – but China is only the seventeenth source with 0.15%.[163] Other sources, however, put China at second place, hosting 12% of attacks, with the US hosting slightly more than a third.[164]

The data illustrate some of China's cyber concerns. China also struggles in its attempt to capitalize on electronic commerce while carefully managing social expectations due to uneven development and challenges to the ruling party's political legitimacy.

Role of the Public Sector – Policy

As a highly centralized state, the Chinese government's role in creating cybercrime policy is paramount, though to date no official strategy appears to have been made public. In addition, unlike Western cyber-security that focuses on the protection of critical infrastructure and communication networks, China's policy view of information security includes concerns about content.[165] Government departments involved in China's cyber efforts include the Ministry of Public Security, the Ministry of Industry, the Ministry of State Security and the military,

---

[161] Latvian Internet Association, *About association,* at http://lia.lv/par_asociaciju. [Document in Latvian]
[162] "China Outlaws Cyber Crime," Strategy Page at http://www.strategypage.com/htmw/htiw/20090524.aspx (accessed 29 January 2012).
[163] Hamadoun I. Touré, "Cybersecurity: Global status update," International Telecommunications Union at http://www.un.org/en/ecosoc/cybersecurity/itu_sg_20111209_nonotes.pdf (accessed 29 January 2012).
[164] Websense Security Labs, "Websense 2010 Threat Report," Websense, Inc at http://www.websense.com/content/threat-report-2010-introduction.aspx (28 November 2011).
[165] Adam Segal, "The role of cyber security in US-China relations," East Asia Forum at http://www.eastasiaforum.org/2011/06/21/the-role-of-cyber-security-in-us-china-relations/ (accessed 29 January 2012).

although the exact nature of each department's role is unknown.[166]

China has not released a formal cyber-security or cybercrime strategy, but its 2006 National Defence White Paper emphasized the country's focus on the "informationization" of the military, which includes the enhancement of cyber-warfare capabilities and improvement and modernization of the military network infrastructure. Within the military, the Third Department (cryptologic services) and Fourth Department (electronic warfare) are considered to be the two leading departments. The Third Department, due to its experience with signal intelligence, is believed to have assumed the responsibility for assuring the security of military computer systems. In 2010 the military disclosed the existence of China's first "Information Support (Assurance) Base", believed to be China's cyber command.[167]

In 2007, China's Ministry of Public Security introduced the Multi-Level Protection Scheme, which required banks, government and infrastructure companies to use security technology provided by Chinese technology firms; the scheme has been increasingly enforced since 2010. The National Computer Network Emergency Response Technical Team Coordination Center of China (CNCERT/CC) is China's national level computer emergency response team, established in 1999. It is responsible for the coordination of activities among all teams within China concerning incidents on national public networks.

Role of the Public Sector – Law

In China, the Public Security Bureau is responsible for internal cyber-security as formally codified in the Computer Information Network and Internet Security, Protection and Management Regulations (1997). Internet service providers in China lack the safe harbour protection enjoyed by their Western counterparts. Providers face cancellation of their business license and network registration, fines, and possible criminal prosecution of company staff for internet security violations by users. In addition, China's content concerns lead to a much higher level of censorship, often directed by the state but enforced by the private sector. The primary cybercrime legislation is Article 285-287 of the Criminal Law (1997), with Hong Kong specific legislation in the Telecommunication Ordinance (Section 27A & 161).[168] The Criminal Law was amended in 2009 to modernize the laws against botnets, Trojans and other modern malware.

In contrast with the harsh penalties imposed by the Chinese criminal system on some offences, such as execution for corruption, Chinese cybercrime law enforcement appears quite lenient. For example, the maximum prison term for intrusion into state systems is three years imprisonment.

[166] Dave Lee, "Israel tops cyber-readiness poll but China lags behind," BBC News at http://www.bbc.co.uk/news/technology-16787509 (accessed 29 January 2012).
[167] Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," Project 2049 Institute at http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf (accessed 29 January 2012).
[168] Stein Schjolberg, "China," Cybercrime Law at http://www.cybercrimelaw.net/China.html (accessed 29 January 2012).

Over the last decade, 102 cybercrime offenders were publicly reported, with only thirteen reported to have received official punishment. In comparison, two thirds of offenders were sentenced in the US over the same period of time.[169]

In late 2011, China's Supreme People's Court and Supreme People's Procuratorate jointly issued a legal interpretation that aims to fight hacking and other internet crimes more aggressively. The interpretation defined relevant terms and clarified criteria for imposing penalties in certain cybercrime cases. The interpretation's purported aim is to tackle such crimes with greater force. The action was seen as part of response to rising cybercrime incidents in China, with the Ministry of Public Security recently estimating eight out of ten internet-connected computers are controlled by hackers.[170]

Role of the Private Sector – For-Profit

China's unique position as a developing country that can translate its scale into significant power is evident in the private sector, dictated in part by the government. China has the largest internet using population in the world with over half a billion users but its penetration rate is still below 40%. This mismatch between sophistication and scale can also be seen in China's recent thirteenth place overall ranking in a report on cyber-power, but the country is the leader in the trade category due to its export-oriented economy.[171]

China is committed to promoting indigenous innovation through the development of national ICT and security standards through various policies, including the Multi-Level Protection Scheme. Some critics argue this may be a protectionist measure, an attempt to leverage security concerns to shut down trade in its growing ICT security products market.[172] Another potential consequence could be a technology transfer by security companies wanting access to the Chinese market. Further, one researcher has noted that China employs massive numbers of external "consultants" to "review" source-code of leading Western software, allegedly in order to find "bugs" but none have ever been publicly reported.[173] In addition to the challenges of foreign companies operating in China, some of China's leading telecommunications manufacturers (Huawei and ZTE) have faced similar security concerns over the possibility of operating in

[169] Michael Yip, "An investigation into Chinese cybercrime and the underground economy in comparison with the West," University of Southampton at http://www.slideshare.net/nicolascaproni/an-investigation-into-chinese-cybercrime (accessed 29 January 2012).
[170] Deng Shasha, "China issues legal interpretation to tighten grip on hacking," Xinhua News Agency at http://news.xinhuanet.com/english2010/china/2011-08/29/c_131082389.htm (accessed 29 January).
[171] Economist Intelligence Unit, "Cyber Power Index: Findings and Methodology," Booz Allen Hamilton at http://www.cyberhub.com/Home/DownloadFindings (accessed 29 January 2012).
[172] Robert McMillan, "China policy could force foreign security firms out," Network World, Inc at http://www.networkworld.com/news/2010/082610-china-policy-could-force-foreign.html (accessed 29 January 2012).
[173] Craig Wright, "Zero days, China's cyber crime," Charles Sturt University at http://news.csu.edu.au/director/latestnews/science.cfm?itemID=AFB646CFE7FBE77D95E5D1396DB4AC4A&printtemplate=release (accessed 29 January 2012).

critical Western networks.

Recently, the Ministry of Industry and Information Technology started working with ten domestic Chinese search engines, including market leaders Baidu and Sohu, and financial institutions to prevent phishing attacks on Chinese web users. The initiative comes after a series of attacks have resulted in a cumulative 45 million online banking accounts being compromised.[174] According to a recent report by Anti-Phishing Working Group, around 70% of all maliciously registered domain names in the world were established by Chinese cyber criminals for use against Chinese companies.[175]

Role of the Private Sector – Not-For Profit

China's not-for profit sector does not appear to play much of a formal role in China's cybercrime strategy. Shortly after the recent legal interpretation of China's cybercrime laws, two prominent Chinese hackers released "Hackers' Self-Discipline Convention", as a moral code that outlines appropriate hacking activities and calls for the rejection of cybercrime.[176] Both currently work within China's IT security industry and previously were "patriotic hackers".

Cooperation with other jurisdictions

China is not a signatory to the Convention on Cybercrime and has instead proposed that the UN serve as the appropriate body to negotiate an international treaty. China has also suggested using the International Code of Conduct for Information Security drafted by China, Russia, Tajikistan and Uzbekistan as an alternative starting point for a cyberspace treaty. Critics of the Code of Conduct are concerned that it could be used to persecute internet-based dissent, while China, and others, are concerned that the Convention on Cybercrime violates international law norms and countries' sovereignty.

While broad multilateral treaties seem a ways off, China has established bilateral police cooperation with nearly thirty countries including the US, UK, and Germany. Between 2004 and 2010 Chinese law enforcement agencies assisted 41 countries with the investigation of 721 cases of cybercrime. China works with regional neighbours in the Asia Pacific region of Interpol and has established the Cybercrime Technology Information Network System (CTINS) with Japan, Republic of Korea, and twelve other Asian countries to exchange information on cybercrimes and share investigation technologies and procedures.[177] Further, China cooperates informally

[174] "Chinese Government taking strong step against Cyber Crime," The Hacker News at http://thehackernews.com/2012/01/chinese-government-taking-strong-step.html (accessed 29 January 2012).
[175] "APWG Report: Cybercrime Attacks on Chinese Businesses Surged in First Half of 2011," Business Wire at http://www.businesswire.com/news/home/20111107006998/en/APWG-Report-Cybercrime-Attacks-Chinese-Businesses-Surged (accessed 29 January 2012).
[176] Michael Kan, "Chinese hackers pledge to reject cybercrime," Computer Crime Research Center at http://www.crime-research.org/news/09.20.2011/3882/ (accessed 29 January 2012).
[177] Gu Jian, "Strengthening international cooperation and joining hands in fighting against transnational cybercrime," China.org.cn at http://www.china.org.cn/business/2010internetforum/2010-11/09/content_21306503.htm (accessed 29 January 2012).

with Taiwanese law enforcement officials on cross-border cybercrime investigations, although these efforts can oscillate according to the larger context of their political relationship.[178]

Conclusion

The following table summarizes the features of the various strategies covered in this report. Somewhat crudely, it attempts to depict whether the role a certain sector plays within a given strategy is significant or minimal, and how far along a country is in terms of the development and deployment of its cyber-security strategy.

Table 1 – A Comparative Snapshot of Strategies Worldwide

Country	Strategy Development	Policy Implementation	Public Sector: Policy	Public Sector: Law	Private Sector: For-Profit	Private Sector: Not-For Profit
New Zealand	*Minimal*	*Modest*	*Significant*	*Modest*	*Minimal*	*Significant*
Australia	*Modest*	*Modest*	*Significant*	*Modest*	*Significant*	*Minimal*
UK	*Significant*	*Significant*	*Significant*	*Modest*	*Significant*	*Minimal*
US	*Significant*	*Significant*	*Modest*	*Significant*	*Significant*	*Modest*
Germany	*Significant*	*Significant*	*Significant*	*Significant*	*Modest*	*Minimal*
France	*Modest*	*Modest*	*Modest*	*Significant*	*Modest*	*Modest*
Romania	*Minimal*	*Minimal*	*Significant*	*Modest*	*Minimal*	*Minimal*
Russia	*Minimal*	*Minimal*	*Modest*	*Minimal*	*Modest*	*Minimal*
Belarus	*Modest*	*Significant*	*Significant*	*Significant*	*Minimal*	*Minimal*
Ukraine	*Significant*	*Modest*	*Minimal*	*Minimal*	*Minimal*	*Minimal*
Estonia	*Minimal*	*Minimal*	*Significant*	*Minimal*	*Modest*	*Modest*
Lithuania	*Modest*	*Minimal*	*Minimal*	*Minimal*	*Minimal*	*Minimal*
Latvia	*Significant*	*Minimal*	*Minimal*	*Significant*	*Minimal*	*Modest*
China	*Minimal*	*Minimal*	*Modest*	*Modest*	*Minimal*	*Minimal*

[178] Yao-chung Chan, "Cyber Conflict Between Taiwan and China," at Australian National University http://asiapacificweek.anu.edu.au/readings/cyberconflict.pdf (accessed 29 January 2012).

Several conclusions can be drawn from the table and from the discussion above. First, the United States, the United Kingdom, and Germany are the current global leaders in the development and implementation of cyber-strategies. As discussed below, that is beneficial for Canada. Second, the US and UK provide for a major private sector role as part of their strategies, whereas Germany tends to place more of an emphasis on the public sector and on a legislative and regulatory framework. Again, this point is discussed below further, in a Canadian context. Third, and as can be expected, countries align themselves in cyberspace according to their geopolitical blocs.

The Council of Europe's Budapest Convention on Cybercrime is the leading multilateral agreement on cybercrime, with 32 countries having ascended to the treaty and another 15 countries that have signed but not yet ratified. Russia is the most prominent member of Council that has not signed the treaty; outside the Council, Japan has not ratified the treaty while China is not even a signatory.

While the Convention is being advanced by many European countries and the United States as the best option to secure international agreement on combating cybercrime, many states have reservations about a treaty they did not have a role in developing. Developing nations and Russia, in particular, believe the UN is the best venue for an international treaty. As discussed above, Russia has proposed an UN-based treaty, but countries that are signatories to the Cybercrime Convention have argued that it serves as the basis for many countries' domestic legislation and that a completely new international agreement will take too long to negotiate.

Although there is broad international support for several sections of the Convention, such as those dealing with cyber-fraud, child exploitation, and the integrity of computers and networks, two areas in particular remain contentious. Article 10, which focuses on offences related to copyright infringement and intellectual property rights is objected to by developing countries and by others that see it serving US corporate interests. Other states, primarily China and Russia, have expressed concerns over Article 32 (b), which allows the law enforcement agencies of one country to access data in another without the explicit consent of the other country's authorities, if the access was lawfully authorized by businesses or individuals in the other country.[179] In addition, some critics suggest that the jurisdictional issues surrounding this Article are not fully resolved, that there should be an obligation on countries to consult each other in every instance instead of the Convention's "where appropriate" and that the Convention should include a mechanism to facilitate law enforcement cooperation outside of formal state contacts.[180] It appears for some, the Budapest Convention goes too far, for others, not far enough.

[179]For discussion on possible alternative global cybercrime treaties see Stein Schjolberg and Solange Ghernaouti-Helie. *A Global Treaty on Cyber-security and Cybercrime: Second Edition.* Cybercrime Law, 2011. http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf

[180]For such criticism see on Armando A. Cottim, *Cybercrime, Cyberterrorism and Jurisdiction: An Analysis of Article 22 of the COE Convention on Cybercrime*, 2 The Future of Law & Technology in the Information Society

Beyond the challenges to the universal adoption of the Budapest Convention, there are some limitations to the agreement itself. First, significant changes to technology and malware have continuously occurred since the Convention was negotiated in the late 1990s. Second, limited resources in both funding and human capital continue to be an issue in both developed and developing states. Aid by other countries, especially by the US, continues to improve cybercrime law enforcement abilities but greater and more coordinated efforts will be needed.

With changes in communication technologies, forms of civic participation have also changed. Many countries that are currently formulating their cybercrime and cyber-security strategy note the need to differentiate between actions on the basis of the perceived objectives of the perpetrators. Most common is the need to distinguish between crime (albeit potentially on a wider scale than offline crime), industrial/governmental espionage, and acts of terrorism or war – whether carried out by government agencies or merely by politically motivated organizations and individuals, as has occurred in the conflicts in Estonia and Georgia in 2007 and 2008 respectively. Of course, as current international strife in Syria and other Arab countries demonstrates, one regime's terrorist is another country's fighter for democracy, further complicating the implementation of an effective strategy. The following section discusses the extent to which, in light of these international constraints, Canada could benefit from the various approaches surveyed above.

Applicability and Fit of Approach to Canada

The following table summarizes the degree of fit and applicability of each country's approach to Canada. Part of that assessment, included in the table, is the degree to which countries are perceived as being under the threat of cybercrime and other cyber-attacks. In addition, the focus of each country's international efforts is included, e.g. whether the relationship with other jurisdictions focuses on collaboration through the Budapest Convention or by some other means. The table provides in such a manner a comparative snapshot of the strategies Canada faces and the degree to which they fit Canadian priorities.

Table 2 – A Comparative Snapshot of Collaborations and Threats

Country	International Focus	Target of Attacks	Compatibility with Canadian Goals
New Zealand	*Quintet; Budapest*	*Minimal*	*Significant*
Australia	*Quintet; Budapest*	*Modest*	*Significant*
UK	*Quintet; NATO Budapest*	*Significant*	*Significant*

(2010) at http://www.ejls.eu/6/78UK.htm

US	*Quintet; NATO; Budapest*	*Significant*	*Significant*
Germany	*Budapest; NATO*	*Significant*	*Significant*
France	*Budapest; NATO*	*Modest*	*Significant*
Romania	*Budapest; NATO*	*Minimal*	*Significant*
Russia	*CIS-RCC; UN*	*Modest*	*Minimal*
Belarus	*CIS-RCC; Eastern; UN*	*Significant*	*Minimal*
Estonia	*CIS-RCC; Eastern; NATO*	*Significant*	*Significant*
Ukraine	*Budapest; NATO; NB8*	*Significant*	*Significant*
Lithuania	*NATO;NB8*	*Significant*	*Significant*
Latvia	*NATO; NB8*	*Modest*	*Significant*
China	*UN*	*Significant*	*Minimal*

The table reveals that Canada is able to cooperate with the majority of the countries surveyed. As mentioned above, the US, UK and Germany have particular insights for Canada to draw upon:

The United Kingdom
The UK's cybercrime strategy can inform Canada on several issues. First, critics note the lack of clear policy responsibility for cybercrime and cyber-security issues. As a result, agencies are created and priorities shift within short timespans. Coordinating the efforts of the private sector actors and the various government agencies remains an on-going challenge.

Second, the UK has a stronger economic development focus for their cyber-security strategy than any other state reviewed, as evidenced by having the Department of Business, Innovation and Skills – which identifies itself on its website as the "Department of Growth" – as the lead government agency responsible for coordinating policy. The Ottawa hi-tech corridor has a strong history of telecommunications research and development. For-profit businesses such as Research in Motion (RIM) are noted for their world-class mobile device security. RIM plays an important role for business and personal information security and is a partner to law enforcement efforts globally (for some of which it has been criticized). Cyber-security could therefore very well play a role within Canada's forthcoming Digital Economy Strategy.

Third, Canada could look, as the UK does, to develop a national cyber-security educational standard. Increasing the availability of qualified cyber-security experts will benefit cybercrime law enforcement agencies while also improving the ability of government and industry to limit the opportunities for cybercriminals to compromise computers and networks.

The United States

As Canada's most important ally, the US international strategy is of crucial importance. The US, as does the UK, highlights the need for qualified professionals. One of the primary challenges facing almost all law enforcement agencies in this report is a shortage of qualified technical experts. The US is looking into K-12 education to enhance fundamental Science, Technology, Engineering and Mathematics (STEM) to help ensure a steady pipeline of qualified candidates for both private and public sector cyber-security. Canada may benefit from a similarly comprehensive educational approach.

The US has also been very proactive in capacity building in developing countries, an area in which Canada has always been active, and in which Canada has traditionally played a major role. In addition to formal treaties such as the Convention on Cybercrime, Canada can benefit from efforts to enhance the legislative and technical capacities of foreign developing states. Relationships developed between law enforcement agencies could help limit cybercrime havens and assist in future cross-border investigations.

Germany

As mentioned above, Germany was recently recognized as having a leading legal and regulatory framework. Canada is currently in the midst of updating its own framework, with some amendments to the Criminal Code already passed, and other bills in parliamentary discussion. Germany appears to have created a balance between the protection of the privacy of its citizens, and the ability to pursue cybercrimes, that Canada may wish to look to as it attempts to achieve a similar balance. Canada should especially study the implications of recent German law enforcement use of malware to ensure an informed policy stance is developed.

Canada has traditionally sought a middle-ground, on a variety of issues, between the European-continental approach and the Anglo-US approach, reflecting perhaps its own history and origins.[181] The German approach, with its emphasis on the role of law and regulation, could serve as a balance to the US and UK approaches and their emphases on the private sector, diplomacy and public policy. All of these are worthy sources for Canada to look at is it formulates its own Canadian approach.

The Canadian Approach

Cooperation with another country, even a close ally, is difficult at the best of times. Each of the three leading countries discussed above offers Canada a unique approach to cyber-security, focusing on different sectors, and formulating distinctive objectives. Cooperation with countries of a different bloc and a different approach to cyberspace is all the more difficult, even in situations where countries face mutual issues such as cybercrime. Such appears to be the case with Russia and its close allies such as Belarus. Indeed, cooperation is next to impossible in

[181] Re data protection see Levin, A. & Nicholson, M.J. "Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground", University of Ottawa Law & Technology Journal, Vol. 2 (2) pp. 357-395 (2005)

situations where one country accuses the other of a form of cyber-warfare, cyber-terror or cyber-espionage, as is often the allegation levelled at China.

Ultimately, these challenges highlight the choice that the Canadian cybercrime strategy must make. Inward-gazing strategies, with a focus on domestic challenges cannot effectively combat external cybercrime. Strategies that attempt external collaboration must compromise on their goals in order to secure international cooperation, or forge a more confrontational approach. Ironically, cooperation is easier to achieve with countries of a similar legal, political and social background, but from which little cybercrime may originate. The countries with which confrontation is "easier" are those from which more cyber-attacks originate, and with which collaboration would, in fact, be more valuable. Effective cooperation with such countries has been elusive due to their differing legal, political and social priorities.

Therefore, Canada must choose between reaching out to nations with the potential to greatly reduce cybercrime and cyber-attacks on Canada, but with which effective cooperation may never materialize, and between cooperation with a group of like-minded nations that will not be as effective in combating cybercrime in the short term. However, the examples set by the leading countries in the Anglosphere, the EU and NATO are rich and promising, and their careful consideration could lead to a more secure Canadian cyberspace.