International Comparison of Cyber Crime

by
Avner Levin (Director)
Daria Ilkina (Research Associate)

March 2013
Table of Contents

Executive Summary ................................................................. 2
Introduction .................................................................................. 3
Background – Unilateral, Bilateral and Multilateral Approaches – A Brief Overview ........... 4
  The United Nations (UN) ............................................................. 7
  The Council of Europe (Budapest Convention) ................................ 8
  The Organisation for Economic Co-operation and Development (OECD) ....................... 9
  The North Atlantic Treaty Organization (NATO) ........................................ 9
  Asia Pacific Economic Cooperation (APEC) ........................................ 9
  The Virtual Global Taskforce (VGT) ............................................. 10
  Strategic Alliance Cyber Crime Working Group (SACCWG) ............................. 11
Country-Specific Analysis ............................................................... 12
  Australia .................................................................................... 12
  New Zealand .............................................................................. 14
  United Kingdom ......................................................................... 16
  United States of America ............................................................ 18
  Federal Republic of Germany ....................................................... 20
  French Republic .......................................................................... 23
  Republic of Finland ................................................................. 24
  Norway ....................................................................................... 27
  Russian Federation ....................................................................... 30
  China ........................................................................................... 33
  Summary ..................................................................................... 35
Cyber-organizations similar to NAV CANADA ........................................ 36
Recommendations and applicability to the Canadian approach ................................. 36
Conclusions .................................................................................. 37
References .................................................................................... 39
Appendix 1. Eleven countries covered in this report (including Canada) on the world map ..... 50
Executive Summary

This report compares Canada’s international partners and several other countries on measures related to cyber-crime. The main findings are as follows:

- Countries distinguish in their policy and strategy documents between cyber-crimes, which are the domain of law enforcement agencies, and cyber-attacks which are increasingly the domain of the military.

- Canada’s international partners have turned their focus from the prevention of cyber-crime to the protection of critical national infrastructure from cyber-attacks.

- In order to cooperate effectively with its allies Canada must also focus on the protection of critical national infrastructure. However, the risk of this focus is the loss of cooperation with non-traditional allies, such as Russia and China, on the prevention of cyber-crimes.

- European countries and the US allow for warrant-less access to electronic information in order to prevent both cyber-crime and cyber-attacks. Other countries do not acknowledge this possibility publicly.

- The need for, and practice of, warrant-less lawful access or warrant-less lawful intercept is moot in Canada, given recent policy decisions to abandon such legislation.

- Countries have not attempted the creation of a ‘Nav-Canada’ type of agency (private-sector, not-for profit) to implement their cyber-security strategies.

- Agencies to combat cyber-crime or cyber-attacks are typically created as an organizational part of the existing law enforcement or military structure.
Introduction

This study is a follow-up to a previous Privacy and Cyber Crime Institute’s research project “Securing Cyberspace: A Comparative Review of Strategies Worldwide”¹ conducted for Public Safety Canada and carried out in November 2011 – March 2012. The report on that research identified the general challenges of developing cyber security strategies in various countries and offered a comparison of the approaches taken around the world to secure cyberspace on national and international levels. This report focuses more on the applicability of the international approaches to the Canadian environment and on any best practices that could help Canada address the issue of combating cyber crime and securing national cyberspace.

Subject to the project’s timeline this report attempts to address not only Canada’s key partners but other countries as well. Thus, the research is focused on ten countries, including European Union (EU) Member States, New Zealand, Australia, Russia, China and the United States. The primary research method is the review and analysis of public policy documents and other non-classified materials.

The report is structured by country, and for each country the following research questions are addressed:

1. Is there, among Canada’s partners, a distinction between cyber-crimes (conducted by traditional criminal elements) and cyber-warfare (conducted by national or quasi-national agencies)?
2. Are Canada’s international partners focused on the prevention of cyber crime or are they focused on cyber warfare?
3. Does the distinction, to the extent that it exists, matter for the formulation of an effective Canadian strategy?
4. Does the distinction have an impact on the use and formulation of a legal framework for, and the actual use of, warrant-less law enforcement activity?
5. What are the best practices employed by Canada’s partners in their approach to combatting cybercrime and how can these be applicable to Canada’s environment.
6. Do cyber organizations similar in scope and mission to Nav Canada exist in other countries, and would such an organization fit and assist Canada’s cyber-security strategy?

Background – Unilateral, Bilateral and Multilateral Approaches – A Brief Overview

In order to set the stage for the discussion of the individual countries that follow it is important to note that most countries do not act unilaterally on issues related to cyber-space (and indeed on any issue with international aspects). However, countries do act traditionally, by definition, on domestic issues within their jurisdiction. Part of the difficulty of formulating cyber-strategies and cooperating in cyberspace is that it is not always clear whether a threat to computers or networks or to personal information is domestic, or international, in origin.

To illustrate this difficulty, consider the following “Origins of Hacks” map, provided by the NCC Group. The map portrays the top ten countries in the third quarter of 2012 that served as the point of origin of an attack on another computer (a ‘hack’ or ‘cyber-attack’). Some of these attacks, no doubt are aimed at computers and networks in other countries, but others are aimed at computers within the country. Each of these countries, and indeed each and every country that participates in cyberspace, faces the same challenge of attempting to formulate courses of action that integrate both domestic authority and international cooperation.

![Map of origins of hacks](image.png)

Figure 1. Origins of hacks based on the data from the 3rd quarter of 2012 (from the latest published report by NCC Group).

---

2 While the positions of the countries on this list change, it is worth noting that United Stated, China and Russia were consistently reported as the top three countries where the most of the cyber attacks originated every quarter of 2012.

With limited domestic resources, ⁴ lack of inter-jurisdictional cooperation, and lack of regulatory enforcement in cyberspace, ⁵ countries have attempted to increase cooperation with other countries and within international treaties. Below is a figure that shows the countries (in scope of this study) that partnered on a bilateral basis to combat cybercrime.

![Diagram showing bilateral agreements and open dialogs between countries to combat cybercrime.](image)

Figure 2. Bilateral agreements and open dialogs between countries to combat cybercrime.

Some of the notable bilateral engagements in combatting cyber-crime referred to in this figure include:

- **United States – Australia:** In 1951 the Australia, New Zealand, United States Security Treaty (ANZUS) was signed to cooperate on military defence matters in the Pacific Ocean. The Treaty is an alliance of three countries built on separate bilateral bonds – one between United States and Australia and another between Australia and New Zealand. Since 1985 New Zealand has been an inactive member of the Treaty and the meetings are being held only between U.S. and Australia’s officials. In 2011 a new clause was added to ANZUS, which specifies that it will also apply to the cyberspace.

---


• **New Zealand – Australia:** New Zealand has recently moved from observer status to membership in Australia’s Counter-Terrorism and Emergency Management Committees. In a recent joint statement it was agreed that *both countries will work together in the cyber incident response area to ensure that networks of national importance remain resilient to cyber intrusions.*

• **New Zealand – United Kingdom:** New Zealand and the United Kingdom are preparing an agreement in which the two countries will share intelligence, research and development on internet offences, and will draw common strategic goals.

• **China – France:** The China-France Joint Working Committee on Information Technology and Communications.

• **United States – China:** bilateral discussions on cooperation in the *Cybersecurity China Institute of Contemporary International Relations* (CICIR, China) and the *Center for Strategic and International Studies* (CSIS, United States) started in 2009 and the respected organizations have held six formal meetings on cyber security since that time. Over the years the parties have reached some areas of agreement and shared views on issues such as risk of “third-party” non-state actors (i.e., terrorist groups), and views on cooperation against cyber crimes such as fraud and child pornography. However, there are still some areas of disputes. For instance, China proposed an agreement on “no-first-use” (i.e., an agreement not to take the first step in cyber-warfare) between major cyber powers and a prohibition of cyber attacks against purely civilian targets. Meanwhile, the U.S. indicated that “the line between civilian and military is blurred, but the concept of the protection of civilians can be found in the Geneva and Hague conventions, which CSIS proposes that all nations agree to observe in cyberspace” Furthermore, the parties discuss what behaviours could be considered cyber attack or cyber war. So far they agreed that the stakes should be high; however, they still need to define the duration and effects of cyber actions that could be regarded as cyber attacks. We have yet to observe what turn the international dialog on cyber security between the two countries will take in light of the recent report from the U.S.-based cyber threat analysis agency Mandiant that exposed a series of cyber attacks from China on United States, the accusations that where later denied by Chinese officials.

---


Furthermore, there is a bilateral China-US engagement “On Cybersecurity Cooperation Against Spam” since 2011. The objectives of this cooperation include: (1) establishing a genuine dialogue between the subject matter experts and stakeholders from the two countries; (2) develop common understanding of each other’s perspectives; (3) agree on international policy for reducing spam in cyberspace.

- **United States – Canada**: cyber security cooperation is part of the action plan *Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness* between the two countries.  

- **United Kingdom – India** Both countries announced in 2013 that the countries will sign an agreement on cyber security issues this year, which should improve personal data protection and increase the stored amount of United Kingdom’s data on Indian servers.

As to international agreements, there are many international bodies that aim to regulate cyberspace. Among the prominent initiatives are that of the United Nations (UN) and the Council of Europe (also known as the Budapest Convention). Most of the European countries are signatories to the Council of Europe Convention on Cybercrime and assign greater focus on multilateral regional alliance rather than on establishing bilateral cooperation with some select countries. The Council of Europe Convention on Cybercrime was the first international treaty that focused on legal procedures to address the acts of criminal behaviour against computer systems and networks. Apart from the 45 members of the Council of Europe, the Budapest Convention has been adopted by Canada, Japan, South Africa and the United States.

**The United Nations (UN)**
The UN attempts to govern cyberspace through the International Telecommunications Union (ITU) and the regulations created by the ITU (ITRs). The United Nations Office for Drugs and Crime (UNODC) is also concerned with cybercrime. ITRs concerning cyberspace were adopted initially in 1988. A resolution on computer crime legislation was adopted in 1990, at the 8th U.N. Congress on the Prevention of Crime and the Treatment of Offenders in Havana, Cuba. In 2000 Resolution 55/63 on combating the criminal misuse of information technologies was adopted by the General Assembly, and it includes the following statements:

- “States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies.”

---

14 ITU 2013: [http://www.itu.int/en/wcit-12/Pages/overview.aspx](http://www.itu.int/en/wcit-12/Pages/overview.aspx)
- “Legal systems should protect the confidentiality, integrity, and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized.”

This was followed by Resolution 56/121 in 2001, and by the launch in 2007 of the Global Cybercrime Agenda (GCA) by the ITU. In 2010 the General Assembly adopted Resolution 65/230 that proposed to establish “an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and responses to it by the Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with the view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime”.

The latest amendments (“Final Acts”) were added to the ITR at the recent World Conference on International Telecommunication held in Dubai in December 2012 (WCIT-12). 89 countries were signatories to the Final Acts. Among the countries covered in this report, only Russia signed the amendments, and the Dubai amendments were widely portrayed as attempts by Russia and its allies to wrest control over the internet from the United States.

The Council of Europe (Budapest Convention)
The Council covers Europe as well as Russia. Canada and the US are Observer States. In 1997 the Council established a Committee of Experts on Crime in Cyber-space, and in 2001 the Council adopted the Convention on Cybercrime, known as the Budapest Convention. Russia objects to certain Convention provisions, which allow for what Russia considers extra-jurisdictional exercises of power that amount to interference in a country’s internal affairs. According to some reports over 100 nations are using the Council of Europe Convention as the basis for domestic legislation to combat the threat of cybercrime. So far 35 countries are a party to the Convention.

Other prominent organizations include the OECD, NATO and APEC.

---

17 Signatories of the Final Acts: 89. [http://www.itu.int/osg/wcit-12/highlights/signatories.html](http://www.itu.int/osg/wcit-12/highlights/signatories.html)
The Organisation for Economic Co-operation and Development (OECD)
The OECD was the first international organization that initiated guidelines for computer crime. By its nature the OECD does not establish treaties, and it is devoted to the promotion of a global coordinated policy approach. The OECD established a Task Force on Spam in 2004. The OECD Working Party on Information and Privacy (WPISP) develops international guidelines on cyber security and in 2002 published a document titled “Security of Information Systems and Networks: Towards a Culture of Security.” In 2008 it released “Scoping paper on online Identity theft” a report with some recommendations on how to fight identity theft (this document also suggested to recognise identity theft as a separate offence in criminal laws.) It was followed up in 2009 by the “OECD Policy Guidance on Online Identity Theft” report.

The North Atlantic Treaty Organization (NATO)
By virtue of its mandate NATO focuses more on cyber-attacks carried by countries or national elements against NATO members. NATO’s Senior Civil Emergency Planning Committee (SCEPC) assists NATO members in the protection of civilian populations from terrorist attacks against critical infrastructure and is also responsible for coordinating the civil critical infrastructure. NATO’s Civil Communication Planning Committee (CCPC) is responsible for the electronic public and non-public communication infrastructures, and has published several papers on civil communications infrastructures. NATO’s Civil Protection committee (CPC) has initiated work on critical infrastructure protection, and developed a Critical Infrastructure Protection Concept Paper in 2003. NATO’s Industrial Planning Committee (IPC) has also contributed on preventive measures for the protection of critical infrastructure. NATO established a Centre of Excellence for Defense against Terrorism in 2008.

Asia Pacific Economic Cooperation (APEC)
The deliberations of APEC are important in this and other multinational areas since it brings together the US, Canada, China and Russia. In 1990 APEC established its Telecommunications and Information Working Group (TEL) that works in turn through three groups: the Liberalisation Steering Group (LSG), the ICT Development Steering Group (DSG) and the Security and Prosperity Steering Group (SPSG). SPSG’s scope covers the promotion of security, trust and confidence in networks/ infrastructure/ services /technologies / applications / e-commerce; oversight of Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs); the issues of Spam, Spyware and Cybercrime prevention; the development of human resources and capacity in order to combat cybercrime and implement effective cyber security awareness initiatives; and the facilitation of business through discussions with the private sector on promoting security, trust and confidence in the use of ICT for business.

---

http://www.cybercrimelaw.net/OECD.html
and trade.\(^{21}\) Of these, the e-Security Task Group created in 2003 a Cybercrime Legislation &
Enforcement Capacity Building Project.

Two other multinational organizations should also be mentioned. The Organization of American
States (OAS) to which both Canada and the US belong, has a Department of Legal Cooperation
that offers an “Inter-American Cooperation Portal on Cyber-Crime”.\(^{22}\) OAS agreed in 2003 to a
“Comprehensive Inter-American Cyber-security Strategy: A multidimensional and
multidisciplinary approach to creating a culture of Cyber-security.”

The Shanghai Cooperation Organization (SCO) is an organization of Russia, China and several
former Soviet republics. These countries have entered into the Shanghai Convention on
Combating Terrorism, Separatism and Extremism. SCO has also issued several related
statements: The Yekaterinburg Declaration of 2009 mentioned information security as one of the
main priorities in a common system of international security. In 2012 SCO’s Heads of State
Council meeting in Beijing stated: “The SCO will stand firm to fight against terrorism,
separatism and extremism as well as international cybercrime”\(^{23}\).

Sometimes international cooperation against cyber crime is established with a very particular
goal and not just on a national level but between specific governmental agencies. An example of
such organization is The Virtual Global Taskforce (VGT)\(^{24}\).

**The Virtual Global Taskforce (VGT)**

VGT is an alliance of international law enforcement agencies and private sector partners working
together to combat online child sexual abuse. Specifically, the VGT comprises the Australian
Federal Police as Chair, the Child Exploitation and Online Protection Centre in the UK, the
Royal Canadian Mounted Police, the US Department of Homeland Security, INTERPOL, the
Italian Postal and Communication Police Service, the Ministry of Interior for the United Arab
Emirates, the New Zealand Police and Europol.\(^{25}\)

One more particularly notable international organization against cyber crime is Strategic
Alliance Cyber Crime Working Group.

---


\(^{23}\) [http://www.fmprc.gov.cn/eng/zxxx/t939149.htm](http://www.fmprc.gov.cn/eng/zxxx/t939149.htm)

\(^{24}\) Virtual Global Taskforce Official Website [http://www.virtualglobaltaskforce.com/](http://www.virtualglobaltaskforce.com/)

Strategic Alliance Cyber Crime Working Group (SACCGW)
SACCGW was assembled in 2006. It is a special unit consisting of five law enforcement agencies (see Fig. 4): The Australian High Tech Crime Centre (AHTCC), FBI (USA), New Zealand Police, Royal Canadian Mounted Police, and Serious Organised Crime Agency (United Kingdom).  

![The Strategic Alliance Cyber Crime Working Group](source)

Figure 3. The Strategic Alliance Cyber Crime Working Group. (Source: FBI.gov).

Over the last five years several countries repeatedly tried to initiate discussion about the need for common international Cyberspace Treaty, suggesting that bilateral and regional agreements are not enough to secure cyberspace and prevent cyber-war.

---

Country-Specific Analysis

This section of the report addresses the country-specific research questions, beginning with Canada’s traditional partners for international cooperation (the “Anglosphere”) and then moving to several other countries of significance in cyber-space.

Australia
In 2012 Norton claimed that more than 5.4 million Australians were victims of cyber-crime – a quarter of the country’s total population; those crimes cost Australia $1.65 billion over that year, and the Australian Government expected cyber-crime costs to stay above $1 billion a year for the foreseeable future.27

Cyber-crime v. Cyber-warfare

*Does the Distinction Exist?*

Both terms “cyber crime” and “cyber attack” are mentioned in Australian policy documents in different contexts; thus, the distinction is apparent, even though there is no clear definition provided for either of the terms.

*Where is the Focus?*

Australian Government's Cyber Security Strategy was launched on 23 November 2009, as an outcome of the E-security Review 2008. The strategy articulates a number of strategic priorities, among which on the first place is “Threat Awareness and Response” set to “improve the detection, analysis, mitigation and response to sophisticated cyber threats, with a focus on government, critical infrastructure and other systems of national interest”. Other priorities include educating the Australians with information and practical tools to protect themselves online, cooperate with businesses to promote cyber security, promote the development of a skilled cyber security workforce, model best practice in the protection of government ICT systems, and promote a secure global electronic operating environment that supports Australia's national interests. “Legal and Law Enforcement” is one of the last objectives identified in Australian Cyber Security Strategy, and it is set to “maintain an effective legal framework and enforcement capabilities to target and prosecute cyber crime”. A new cyber security centre will be established in Australia by the end of 2013.28

---


In our opinion, this order of priorities indicates that the main focus of the Australian Government is at securing the national critical infrastructure and people from cyber attacks.

The Law and the need for Warrants
The Ministry for Home Affairs and Justice and the Police are the authorities responsible for cyber-crimine. The Ministry released the Protocol for Law Enforcement Agencies on Cybercrime Investigations in 2011. The protocol provides a cyber-crimine investigation matrix that outlines the most appropriate agencies to deal with particular types of complaints, and provide specific arrangements for sharing information to cyber crime investigations between jurisdictions.\(^\text{29}\)

The Cybercrime Act states the following offences:

- 477.2. Unauthorised modification of data to cause impairment: 10 years imprisonment.
- 477.3. Unauthorised impairment of electronic communication: 10 years imprisonment.
- 478.1. Unauthorised access to, or modification of, restricted data: 2 years imprisonment.
- 478.2. Unauthorised impairment of data held a computer disk: 2 years imprisonment.
- 478.3. Possession or control of data with intent to commit a computer offence: 3 years imprisonment.
- 478.4. Producing, supplying or obtaining data with intent to commit a computer offence: 3 years imprisonment.\(^\text{30}\)

Australia acceded to the Budapest Convention and new law enforcement measures had to be introduced as part of the joining the Convention, the Cybercrime Legislation Amendment Bill, which came into force in Fall 2012.\(^\text{31}\) One of those measures will allow other countries on the Council to serve notices to Australian ISPs requiring them to store 180 days of web data for targeted users, and at a later stage the foreign countries can obtain a warrant to take receipt of the recorded information. Further changes have been proposed but not yet implemented, perhaps for political reasons.\(^\text{32}\)

---


30 It is worth noting that every computer related crime is punishable by imprisonment; there is no mention of alternative penalties such as paying a fine.


The expected changes include extending the period of time between interception and obtaining a warrant, mandatory data retention, surveillance of social networks, and criminalization of encryption. Under the proposed law, ISPs, search engines and social networks, and other websites are required to store all the information for 2 years, which could be accessed without a warrant by the Australian Security Intelligence Organization (ASIO). ASIO will have a right to demand personal passwords to access this data and to deny providing this information would be illegal. Moreover, ASIO would also have a legal right to access any computer without a warrant if that computer is somehow connected to the computer of a person who’s being suspected of a crime.  

**New Zealand**

According to 2010 data, 70% of New Zealand adults have been the targets of some form of cyber-crime, with the most common complaints being computer scams, fraud and viruses/malware.

**Cyber-crime v. Cyber-warfare**

*Does the Distinction Exist?*

The difference between “cyber-crime” and “cyber-attack” is defined in New Zealand’s Cyber Security Strategy as follows:

Cyber-attack – *An attempt to undermine or compromise the function of a computer-based system, access information, or attempt to track the online movements of individuals without their permission.*

Cyber-crime (or computer crime) – *Any crime where information and communication technology is: 1) used as a tool in the commission of an offence; 2) the target of an offence; 3) a storage device in the commission of an offence.*

In New Zealand some of the most common examples of cyber-crime include fraud, identity theft and organised crime.

*Where is the Focus?*

The distinction between cyber-crime and cyber-attacks was important in formulating the Cyber Security Strategy. A cyber-attack can be classified as a computer or cyber-crime, yet from New Zealand’s Cyber Security Strategy it is evident that the following cyber threats require a special

---


response and are more serious than domestic crimes: cyber-espionage, hacktivism and terrorist use of the Internet. The highlighted difference from regular cyber-crimes is that the targets of these attacks are not individuals or private organizations, but government systems, critical national infrastructure and “businesses that have resulted in access to commercially sensitive information, intellectual property and state or trade secrets”. Therefore, the Cyber Security Strategy is formulated particularly with the key objectives “to improve the level of cybersecurity across government [and] for critical national infrastructure and other business”. Protecting government systems and information is one of the main priorities in addition to increasing awareness about cyber threats and improving incident response and planning.

The Law and the need for Warrants
The following offences are identified as “crimes involving computers” and are subjected to punishment according to Crimes Act:

- **Section 249** – “Accessing computer system for dishonest purpose”:
  - Every one is liable to imprisonment for a term not exceeding 7 years for accessing computer system, dishonestly or by deception, in order to obtain any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or to cause loss to any other person. The intent to access computer system is also punishable – by imprisonment for up to 5 years.

- **Section 250** specifies imprisonment for a term not exceeding 10 years to everyone who intentionally damages or alters any computer system “if he or she knows or ought to know that danger to life is likely to result”. Any damage to computer system, interference with data without authorisation, causing computer system to fail or deny service to any authorised user is punishable by imprisonment for up to 7 years.

- **Section 251** Making, selling, or distributing or possessing software for committing a crime – imprisonment for up to 2 years.

- **Section 252** Accessing computer system without authorisation – punishable by up to 2 years of imprisonment.

Similar to Australian legislation, every computer related crime in New Zealand is punishable by imprisonment, and there is no mention of any alternative penalties, e.g. paying a fine.

In 2012 New Zealand passed the Search and Surveillance Act. The Act unified the powers that previously were scattered across roughly 70 agencies. The Secret Intelligence Service and the Government Communications Security Bureau are still governed by their own legislation.

Under the Act police can complete some forms of surveillance and searches without warrants.

---


but only in emergency situations where either life could be at risk or there is a risk of destruction of evidence.\textsuperscript{37}

United Kingdom

Cyber-crime v. Cyber-warfare

\textit{Does the Distinction Exist?}

The policy documents we reviewed do not offer explicit definitions for cyber-crime, cyber-attack or cyber warfare. However, the distinction is clearly present.

In the Parliamentary Office of Science & Technology’s report “Cyber Security in the UK” two types of cyber attacks are discussed – attacks on information infrastructure and attacks on physical infrastructure; it is briefly explained that cyber attacks are “aimed to steal sensitive information and data from financial, government and utilities infrastructure targets”.\textsuperscript{38}

The Ministry of Defence comments on the emerging discussion about cyber war: “There is an ongoing and broad debate regarding what ‘cyber warfare’ might entail, but it is a point of consensus that with a growing dependence upon cyber space, the defence and exploitation of information systems are increasingly important issues for national security. We recognise the need to develop military and civil capabilities, both nationally and with allies, to ensure we can defend against attack, and take steps against adversaries where necessary.”\textsuperscript{39}

\textit{Where is the Focus?}

The UK’s Cyber Security Strategy 2011 provides the action plan for the country to meet these objectives by 2015, in the order of importance:

1) The UK to tackle cyber crime and be one of the most secure places in the world to do business in cyberspace.

2) The UK to be more resilient to cyber attacks and to be better able to protect the UK’s interests in cyberspace.

3) The UK to have helped shape an open, stable and vibrant cyberspace, which the UK public can use safely and that supports open societies.

4) The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all British cyber security objectives.\textsuperscript{40}


\textsuperscript{38} POST Note No 389, 2011 – Cyber Security in the UK. Available for download from \url{http://www.parliament.uk/mps-lords-and-offices/offices/bicameral/post/publications/postnotes/}.


Therefore, we can see that the British government puts greater emphasis on combatting cybercrime, while the objective to protect the country from cyber attacks comes second. It’s been estimated that the UK economy suffers from a loss of £27 billion (CAD $42.11 billion) due to cyber crime, annually. In March 2013, announcing that cyber threat became “more complex”, the British government created a new cyber-crime unit, that has already made 19 arrests and frozen about £500,000 in assets.

The objective to secure the UK from cyber attacks is also taken seriously. In 2010 the Government invested £650 million in a four-year National Cyber Security Programme (NCSP) (see Fig.4). Around half of this funding was assigned towards enhancing the UK’s core capability to detect and counter cyber attacks. This “core capability” is mainly concentrated in the intelligence agency GCHQ, headquarters in Cheltenham, Gloucestershire. The UK Cyber Security Strategy 2011 reported on this investment: “The details of this work are necessarily classified, but it will strengthen and upgrade the sovereign capability the UK needs to confront the high-end threat”.

The Law and the need for Warrants

The Computer Misuse Act (1990) describes different computer misuse offences and outlines penalties for them: (1) unauthorised access to computer material; (2) unauthorised access with

---

42 Quotes and figures in this and the previous sentences are from the Financial Times article of March 14, 2013, written by Hannah Kuchler – “UK launches unit to tackle cyber crime”. [http://www.ft.com/intl/cms/s/0/86c9631a-8c9e-11e2-8ee0-00144feabcde.html#axzz2OldMqppv](http://www.ft.com/intl/cms/s/0/86c9631a-8c9e-11e2-8ee0-00144feabcde.html#axzz2OldMqppv)
43 GCHQ. [http://www.gchq.gov.uk/AboutUs/Pages/index.aspx](http://www.gchq.gov.uk/AboutUs/Pages/index.aspx)
intent to commit or facilitate commission of further offences; and (3) unauthorised modification of computer material. The penalties vary from a fine to imprisonment from six months to ten years depending on nature of the crime. The Act was expanded in 2006.

The Regulation of Investigatory Powers Act 2000 provides a whole chapter on communications interception, including the section on “Lawful interception without an interception warrant” (Chapter I, Section 3). According to this section, communication may be intercepted without a warrant if just one person involved in the communication has consented to the interception; surveillance by means of this interception is authorized as well; communication interception is also authorized if it’s related to “the prevention or detection of anything which constitutes interference with wireless telegraphy”.

In 2012 the Home Office drafted a new Communications Data Bill, which would authorise the state to monitor internet communications and require communications companies to store users’ online history data for twelve months. Currently, the law allows access to a web user’s private information that provides the location of a mobile phone or the identity of a user. The UK government made almost 500,000 requests for access to such information in 2011. The Minister of Security and the police claim that the proposed new bill will be essential in detecting cyber crime; however, the Liberal Democrats oppose the adoption of the bill, saying that it could breach civil liberties.

United States of America
The United States ratified the Council of Europe Convention on Cybercrime in 2006.

Cyber-crime v. Cyber-warfare
Does the Distinction Exist?
In various legal, strategic and academic documents of United States the terms cyber-crime, cyber-attack, computer attack, electronic attack, and cyber-terrorism are coined and defined.

Where is the Focus?
The Department of Homeland Security operates the National Cyber Alert System and the National Cyber Response Coordination Group – two important programs in protecting U.S. from cyber threats. In addition, Homeland Security oversees an ongoing security exercise Cyber Storm.

The National Cyber Security Division (NCSD) is a Department of Homeland Security responsible for protecting cyber infrastructure. To secure cyberspace, NCSD identified two objectives:

1) To build and maintain an effective national cyberspace response system.
2) To implement a cyber-risk management program for protection of critical infrastructure.

The United States Cyber Command (USCYBERCOM or CYBERCOM) was established in 2009 and is a sub-unified command subordinate to U.S. Strategic Command (USSTRATCOM). Service Elements include Army Forces Cyber Command (ARFORCYBER); 24th USAF; Fleet Cyber Command (FLTCYBERCOM); and Marine Forces Cyber Command (MARFORCYBER). The Mission Statement of USCYBERCOM states that the Command “plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.”

The Cybersecurity Strategy for the Homeland Security Enterprise identified two strategic focus areas for the future of cyberspace security: “Protecting Critical Information Infrastructure,” and “Strengthening the Cyber Ecosystem.”

Additionally, the Department of Defense (DoD) in its Strategy for Operating in Cyberspace (adopted in July 2011) described the following five strategic initiatives for U.S. in cyberspace:

- **Strategic Initiative 1**: Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace’s potential.
- **Strategic Initiative 2**: Employ new defense operating concepts to protect DoD networks and systems.
- **Strategic Initiative 3**: Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy.

---

Strategic Initiative 4: Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity.

Strategic Initiative 5: Leverage the nation’s ingenuity through an exceptional cyber workforce and rapid technological innovation.56

Generally speaking, the main focus of the American Government is to protect the U.S. from cyber attack, and the responsibility for this is assigned exclusively to the military.

The Law and the need for Warrants
Cybercrime laws are covered in the Title 18 of the United States Code (18 U.S.C.), which is the Criminal and Penal Code of the United States. 18 U.S.C. sets the penalties for online identity theft, hacking, intrusion into computer systems, and child pornography.57

The Electronic Communications Privacy Act of 1986 and describes requirements for disclosures of data, conditions for mobile tracking devices and surveillance, and interception of communication data.58 It covers interception of wire, oral, or electronic communication and the preservation and disclosure of stored wire and electronic communication. In 1994 the US further modernized its lawful intercept capabilities by passing the Communications Assistance for Law Enforcement Act.

All of the above require judicial supervision. However, since 2001 the US has engaged in warrantless intercepts under its Foreign Intelligence Surveillance Act. The Act withstood scrutiny in 2013.59

Federal Republic of Germany
Germany ratified the Council of Europe Cybercrime Convention in 2009.60

Cyber-crime v. Cyber-warfare
Does the Distinction Exist?
The penalties for cyber-crimes are highlighted in the Criminal Code, but there is no direct mention or definition of the term “cyber-crime” there. However, cyber-crime is discussed (but

---

59 http://www.reuters.com/article/2013/02/26/us-usa-court-surveillance-idUSBRE91P0JS20130226
not clearly defined) in the German Cyber Security Strategy of 2011. It is mentioned there that national capabilities to combat cyber-crime “must be strengthened”, and in order to do it the government “will make a major effort to achieve global harmonization in criminal law based on the Council of Europe Cyber Crime Convention.”

“Cyber-attacks” are defined also in the German Cyber Security Strategy:  
A cyber-attack is an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security. The aims of IT security, confidentiality, integrity and availability may all or individually be compromised. Cyber-attacks directed against the confidentiality of an IT system, which are launched or managed by foreign intelligence services, are called cyber-espionage. Cyber-attacks against the integrity and availability of IT systems are termed cyber-sabotage.”

Where is the Focus?  
The clear definition of cyber-attacks is important in the formulation of Germany’s Cyber Security Strategy, according to which, the government of Germany recognizes that cyber-attacks “may have a considerable negative impact on the performance of technology, businesses and the administration and hence on Germany’s social lifelines” and acknowledge that the threat may come not only from abroad (foreign/external cyber threat) but also from within the country (internal threat), and that it is very difficult to track the origin of a cyber-attack.

Cyber security is a part of Germany’s preventative security strategy, while the main priority is the protection of critical information infrastructures. The German strategic approach is focused on coordination and information sharing between private and public sectors of the country, and also on coordination with foreign and international security policies – in particular, cooperation with the United Nations, EU, the Council of Europe, NATO, the G8, the OSCE and other multinational organizations.

In general, both Criminal Code and the Cyber Security Strategy pay special attention to espionage and sabotage, which are identified as types of cyber-attacks in the Cyber Security Strategy. Based on these documents, we can infer that Germany is more focused on protecting the country from cyber attacks than on preventing cyber crime.

The Law and the need for Warrants  
The German Criminal Code (as amended in 2009) lists the following:  

---

61 Here and further in Part 4.5 of this report the quotes are from Germany’s latest Cyber Security Strategy (edition February 2011), available for download from Federal Ministry of Interior webpage:  
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile, or from ENISA:  
62 Translation of the German Criminal Code to English provided by Prof. Dr. Michael Bohlander for the German Federal Ministry of Justice, and available via this link:  
• Section 202a – Data espionage: Imprisonment not exceeding three years or a fine for unlawfully obtaining data or for unauthorised access to data (Subsection 202a(2) specifies in this and further presented in this report Sections from the Criminal Code that the implied data is “stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable”).
• Section 202b – Phishing: Imprisonment not exceeding two years or a fine for data interception.
• Section 202c – Acts preparatory to data espionage and phishing: Imprisonment not exceeding one year or a fine.
• Section 303a – Data tampering (unlawfully deleting, suppressing, rendering unusable or altering data): imprisonment not exceeding two years or a fine. The attempt is punishable too.
• Section 303b – Computer sabotage: imprisonment not exceeding three years or a fine if the damage is done to another person; imprisonment not exceeding five years or a fine if the damage is done to another business, enterprise or a public authority. In especially serious cases (if offender causes major financial loss, acts on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage, or through the offence jeopardises the population’s supply with vital goods or services or the national security of the Federal Republic of Germany) penalty is imprisonment from six months to ten years.

In 2010 the Constitutional court of Germany overturned a law from 2008 that required telecom companies to keep communications data (logs of calls, faxes, SMS messages, e-mails and history of internet use) for six months. The law was based on the European Union Anti-terrorism Directive, and the discussion to overturn it occurred because many German citizens were against this legislation fearing that their privacy would be invaded. To the law wasn’t overturned completely though, despite that it’s not allowed anymore to record telephone calls or read electronic communication messages, the retention of data is still permitted. The records would include evidence of who got in touch with whom, for how long and how often – without requiring any evidence of wrongdoing.

A new amendment to Telecommunication Act will oblige service providers with more than 100,000 customers to allow the Federal Network Agency to automatically access data on behalf of investigative agencies without the knowledge of providers, while smaller providers will have to answer such requests within six hours. The amended has been criticized that it is not

supported by the German constitution, and it also may undermine the rights of people to privacy and the protection of personal data that are defined under international EU legislation.\textsuperscript{65}

\textbf{French Republic}
The increase of cybercrime in France is most often explained with the constant increase of internet users and with the observable fact that cybercriminals are continuously evolving from being single individuals to becoming a complex interconnected network, forming communities to exchange expertise and knowledge on how to conduct cybercrimes and attacks efficiently.

France ratified the Council of Europe Convention on Cybercrime on January 10, 2006.

\textbf{Cyber-crime v. Cyber-warfare}
\textit{Does the Distinction Exist?}
Cybercrime is defined in France’s Information Systems Defence and Security Strategy (2011) as “Acts contravening international treaties and national laws, targeting networks or information systems, or using them to commit an offence or crime.”

“Cyber-attack” is defined in the 2008 French White Paper on Defence and National Security as a major attack, external or internal, against information systems. Cyberterrorism and cyberwarfare are also mentioned in the White Paper as major threats that need to be not only prevented, but also a response to such actions should be designed.\textsuperscript{66}

\textbf{Where is the Focus?}
France’s Information Systems Defence and Security Strategy lists and explains four strategic objectives of the county in cyberspace:

1) Become a cyber-defence world power in cyber-defence.
2) Safeguard France’s ability to make decisions through the protection of information related to its sovereignty.
3) Strengthen the cyber-security of critical national infrastructures.
4) Ensure security in cyberspace (this involves raising public awareness and understanding of cyber threats, improving policies, detect and block cyber attacks, and develop international collaboration initiatives).

The strategic focus of the country is clearly directed on retaining France’s areas of sovereignty, protecting important businesses and government from espionage on the scientific, economic and commercial assets, protecting the nation from computer attacks. The 2008 French White Paper

\textsuperscript{65} Albertazzle, S. (2012, March 17). \textit{German high court delivers mixed verdict on lawful access rules}. Steptoe & Johnson LLP.
on Defence and National Security explains that “large-scale cyber-attacks on national infrastructures” is the biggest threat France would face over the next 15 years, which led to the development of the Information Systems Defence and Security Strategy specifically focused on the national defence capabilities and measures to be taken to strengthen cyber-defence.

The Law and the need for Warrants
The Penal Code of France (amended 2005) outlines the following crimes:  
- Unauthorised Access to Automated Data Processing Systems – Article 323.
- Violations of Personal Rights Resulting from Computer Files or Processes – Article 226.
- Child pornography – Article 227.

In 2011 France adopted a law that obliges ISPs and social networks to store personal data of the internet users for a period of one year. The information includes “who people are, where and when they go on the Internet, and what they are doing.”

Similar to the other European Member States, France is in compliance with the EU Directive on Lawful Intercept, and has entered into a dispute with Skype over that company’s compliance.

Republic of Finland
Because of its inability to “respond to a large-scale cyber-attack against several vitally important targets at the same time,” Finland saw a need to establish a cyber-security centre that will improve this situation. The new Cyber Security Strategy that was adopted in early 2013 declares that a Security Committee “will be set up to play an active role in the field of comprehensive security [and] will act as a permanent cooperation body for contingency planning”.

In 2012 Finland was assessed and ranked as being one of the top three countries that are most resilient to cyber attacks, alongside with Israel and Sweden. The Defence Minister of Finland

---

67 Cybercrime Laws: France. [http://www.cybercrimelaw.net/France.html](http://www.cybercrimelaw.net/France.html)
72 Helsingin Sanomat, news report from 10/01/2012 – “Finland plans to set up national cyber security centre”: [http://www.hs.fi/english/article/Finland+plans+to+set+up+national+cyber+security+centre/1329104867405](http://www.hs.fi/english/article/Finland+plans+to+set+up+national+cyber+security+centre/1329104867405)
announced that the country aims “to become a global forerunner in cyber-security by 2016.”

Following this statement, the country’s first cyber security strategy was prepared. Prior to this document, the basic strategic goals and security measures of Finland in cyberspace were outlined in Security Strategy for Society (2010). The new Cyber Security Strategy sets cyber security guidelines and management approach, and stresses on the role of government and that the cooperation with private sector is essential, because most of the Finnish critical infrastructure is privately owned.

Cyber-crime v. Cyber-warfare

Does the Distinction Exist?

In the Criminal Code of Finland neither the term “cyber-crime” nor “cyber-attack” are used, however there are “data and communications offences”. Payment card fraud and identity theft are a separate criminal offence. Foreign organised crime groups specialising in payment card fraud have been detected in Finland on a monthly basis since 2009 – either using stolen cards or stealing data from payment cards.

The new Cyber Security Strategy explains that a “cyber-attack can be used as a means of political and economic pressure; in a serious crisis pressure can be exerted as an instrument of influence alongside traditional means of military force,” and clearly states that securing cyberspace against cyber-attacks is the responsibility of the military (Finnish Defence Forces), whereas “the police are the competent authority for carrying out investigations related to cyber-crime”.

Lukin (2012) suggested re-examining Finnish legislation to provide the country with an option to engage in cyber-war – to use cyber attack in case of cyber conflict; some concerns where expressed about the fact that current legislation doesn’t permit the usage of cyber attack against other countries as part of national protection.

Where is the Focus?

It is clear from the new Cyber Security Strategy that the Finnish government attributes a great importance on securing the key businesses, crucial governmental institutions and critical infrastructure providers from cyber-attacks that pose political or economic threat than on solving cyber-crime or enforcing legislation. The main priority is to prepare for exceptional

---


circumstances such as a nation-wide cyber-crisis. The Cyber Security Strategy outlines the responsibilities of current and to-be-established legislative authorities and emphasizes the cooperation between different private and public sectors to secure cyberspace and prepare for effective crisis management. However, the Cyber Security Strategy is not meant to establish laws or set any legal framework; its purpose is to outline the national strategic vision. The Strategy defines the key goals and guidelines, which are used in responding to the threats against the cyber domain and ensure that the Strategy’s objectives are being met.\textsuperscript{80}

The Government Resolution on National Information Security Strategy (2008) says that ‘by 2015 Finland will be the leading country in the world in terms of information security’ and defines the following priorities:

- Priority 1: Basic skills in the ubiquitous information society.
- Priority 2: Information risk management and process reliability.
- Priority 3: Competitiveness and international network cooperation.

There is a criticism among Finnish academics that Finland cannot develop uniform objectives in IT security, because IT security leading is decentralized.\textsuperscript{81} Prior to the 2013 Strategy document the only document comparable in scope was the 2008 Information Security Strategy, which didn’t set an objective to protect national infrastructure from potential cyber-attacks or provide any guidelines on how to respond to one or what authorities should be responsible for national cyber security.

Finland doesn’t have methods developed that would be able to recognize large scale attacks against critical infrastructure, which is probably why over the past year the focus of the government shifted from combatting cybercrime to making an effort in planning how to protect the country from cyber-attacks.

\textit{The Law and the need for Warrants}
In Finland’s Criminal Code criminal offences committed to computers or using computer technology are outlined as follows:

- Chapter 34 – Endangerment
  - Section 9a – Endangerment of data processing
  - Section 9b – Possession of a data system offence device
- Chapter 38 – Data and communications offences
  - Aggravated message interception (imprisonment for at most three years)
  - Aggravated interference with communications (imprisonment for at least four months and at most four years)

\textsuperscript{80} Ministry of Defence of Finland – Press Release of 01/24/2013.
Online surveillance in Finland was increased shortly after the tragic Breivik shooting in Norway. Police were ordered to actively monitor the Internet for evidence of extremist plots. Following an earlier 2008 shooting in Finland a special program was launched in 2009 to put a so-called “blue button” on any webpage – a sign that should alert authorities that a possible criminal behaviour (or rather intention of such behaviour) has been detected on that page.

The relevant legislation is the Police Act (2005), the Act on the Processing of Personal Data by the Border Guard (2005), the Customs Act (1994), and the Coercive Measures Act (2008). According to the Act on the Processing of Personal Data by the Police, the Police may obtain and record (in the special Data System for Police Matters) some personal data without a warrant in the immediate course of an investigation, or in case of a missing or deceased person. There is no mention of surveillance and access to communication data without a warrant if a person is not suspected of a crime or there is no emergency/urgency or danger at stake.

Police are entitled to receive from a telecommunications operator:
1) identification data on transmissions to a particular subscriber connection, with the consent of the injured party and the possessor of the subscriber connection, necessary for the purpose of investigating a violation of a restraining order or breach of domestic peace; and
2) identification data on messages transmitted from a particular mobile communications device, with the consent of the subscriber or owner of the device, insofar as necessary for investigating a crime where the mobile communications device or the subscriber connection used therein has been unlawfully in the possession of another party.

Norway
The Budapest Convention on Cybercrime was ratified by Norway in 2006.

45,000 cyber-crimes were committed in Norway during 2012. The most targeted sectors in 2012 were military defence, oil and gas, energy, government and hi-tech industry. It’s been estimated that Norwegian companies lost about NOK 20 billion (CAD $3.53 billion) because of cyber-

---

82 The information is from the Unofficial English translation of The Criminal Code of Finland. The Ministry of Justice of Finland is using this translation and the document was retrieved from the Ministry’s website. Full text available for download via link: http://www.finlex.fi/en/laki/kaannokset/1889/en18890039.pdf.
83 Ojala (2010)
crimes. However, not all of the cyber-crimes are being reported, because companies are often unaware of the attacks on their businesses.  

Cyber-crime v. Cyber-warfare

Does the Distinction Exist?
The terms “cyber-crime” and “cyber-attack” are not defined in Norwegian law or in Norway’s National Strategy for Information Security (Nasjonal strategi for informasjonssikkerhet). However, the term “computer crime” appears in the National Strategy for Information Security, and “warfare against critical infrastructure” is discussed. The Strategy was adopted in 2012.

Where is the Focus?
The second chapter of the Strategy discusses the importance of ICT infrastructure and the challenges in protecting ICT systems from breaches and unlawful use. One of the paragraphs mentions that “warfare against critical infrastructure” is being developed in many countries, and that it must be assumed that this warfare is sophisticated enough to pose a major threat to the national critical infrastructure. It must be assumed that the attack will be directed against information resources, including computer systems that control critical infrastructure and industrial processes. While emphasizing that international cooperation on information security is essential, it is also accentuated in the document that a country must safeguard its own national interests in the ICT area.

To protect the country from cyber threat, the main recommendation in the Strategy for Information Security is to continuously raise awareness among businesses and individuals that such threat exists, and increase competence on how individuals and businesses can secure their computer systems.

Other measures include continuing support for the Norwegian National Security Authority (Nasjonal sikkerhetsmyndighet or NSM), which is a “cross-sectorial professional and supervisory authority within the protective security services in Norway” that defines protective security as actions that are aimed “to counter threats to the independence and security of the realm and other vital national security interests, primarily espionage, sabotage or acts of terrorism”. The NSM was established in 2003 and is responsible for the Security Act; Defence Secrets Act; Defence Inventions Act; the certification of information systems and products (SERTIT); coordinating role in preventative work and responses against IT security breaches aimed at vital infrastructure in Norway (NorCERT); and, developing the Norwegian Computer Network Defence (CND) strategy.

---


The Law and the need for Warrants

The Norwegian General Civil Penal Code (2005) does not define cyber or computer crimes and the word “computer” does not even appear in the Code. Instead, the terms “electronic means”, “technical devices” and “technical equipment or software” are used. Below are the sections from the Civil Penal Code that can be interpreted as applying to cyber crime:

- Chapter 13 – Felonies Against the General Order and Peace
  - Section 145. Unlawfully obtaining data or software (fines and/or imprisonment for up to 6 months)
  - Section 145b. Making available to others someone else’s passwords or other data that can provide access to a data system (fines and/or imprisonment for up to 6 months)
  - Section 151b. Any person who by destroying, damaging, or putting out of action any data collection or any installation for supplying power, broadcasting, electronic communication, or transport causes comprehensive disturbance in the public administration or in community life in general shall be liable to imprisonment for a term not exceeding 10 years.

- Chapter 24 – Embezzlement, Theft, and Unlawful Use
  - Section 262 creating, distributing, possessing, installing, or attempting these actions with a decoding device for unauthorized access to a protected [telecommunications] service.

- Chapter 26 – Fraud, Breach of Trust and Corruption
  - Section 270 – altering data or software or the result of automatic data-processing (fines or imprisonment for up to 3 years)

A Bill was suggested as an amendment in 2009, introducing a passage on “Identity Infringements”, and indicating that identity theft shall be punishable with a fine or imprisonment for a term not exceeding 2 years. This Bill is not part of the Code yet.

According to the Criminal Procedure Act (1981), communications surveillance requires a court order. If there is a great risk that the investigation will be impaired by delay, an order from the prosecuting authority may take the place of a court order (Section 216 d).

---

88 Note that some countries classify such offences as cyber-attacks.
89 Cybercrimelaw.net. (2013). Latest news on Cybercrime legislation from around the world: http://www.cybercrimelaw.net/Cybercrimelaw.html
90 Council of Europe’s Committee of Experts on Terrorism (CODEXTER), 2007.
Russian Federation
The authority in charge of solving cyber-crimes in Russia is Department “K” of the Ministry of Internal Affairs of the Russian Federation (Russian: Ministerstvo Vnutrennikh Del or MVD). In late 2012 MVD published their latest report with statistical data on crimes in high technologies (covering the first half of the 2012). The data indicates that for that period 5696 cyber-crimes were detected in Russia, up by almost 11% compared to the same period from 2011.

The leading Russian computer security company Group-IB states two reasons for the rapid and continuous increase in cyber crimes in Russia. First, the legislative system to combat cyber-crimes is ineffective and the punishment for cyber-crimes in Russia is very mild: the sentences for computer related crimes are either very short or suspended. Second, different hacker organizations try to cooperate with each other to get higher profits and support their criminal enterprises.

The most popular cyber-crimes in Russia are:
1) various online fraud activities (stealing funds from bank accounts, phishing, SMS text messages scams, stealing payroll records using viruses, etc.),
2) spam distribution
3) DDoS-attacks.

Cyber-crime related to child pornography is a topic of special attention in Russia. In 2011 the government launched a nationwide program “Sornyak” to combat with this particular type of crime. The program is still ongoing; as a result of the investigations conducted within this program, by September 2012 the authorities instituted 131 criminal proceedings on the basis of material obtained in the course of the operation “Sornyak”. Based on the efforts of the “Sornyak” program the international cooperation of 24 countries, including Russia, has been established to fight child pornography. Canada is among the participating countries alongside with the US, UK, Australia, Germany, Belgium, and Netherlands.

Cyber-crime v. Cyber-warfare
Does the Distinction Exist?
Russian and Chinese authorities often use the term *informationization* in their strategic and policy documents, which means “the intensive exploration and use of information resources for social and economic development”. In Russia, the word “cyber” is generally used only in media and academic publications. In the official policy documents the words “information” or “informational” are most often used instead as in *information security*, *informational resistance*, *information space* (instead of *cyberspace*), etc.

Even though the terms “cyber-crime” and “cyber-warfare” or “cyber-attack” do not appear in any of the official public documents, the use of terms such as “information security”, “computer information crime” or “computer crime”, and “informational resistance” (discussed below), makes it clear that the government distinguishes between regular cybercrimes and cyber-warfare (“information warfare”).

 Where is the Focus?
The Doctrine on Information Security of the Russian Federation (2000) is the main document that outlines Russia’s national interests in the information area, which are:

1) Protection of the individual constitutional rights and freedoms related to obtaining and use of information.
2) Raising awareness (international and within the country) about Russia’s information policy.
3) Development of modern information technologies and information industry in the country.
4) Protection of information resources from unauthorized access, ensuring the security of information and telecommunication systems that are already deployed or just being set up in Russia.

It is clear that the main focus of this document is the digital disparity in Russia, or the accessibility of ICT infrastructure.

In 2010 a new Military Doctrine was published in which great importance was assigned to information security (securing the objects of informational infrastructure and strengthening informational resistance). From this Doctrine it is clear that ensuring national cyber security is the responsibility of the military. The Military Doctrine defines different types of the modern military conflicts and states that information resistance is one of the characteristics of such conflicts. It also explains that attacks on the objects of informational infrastructure are major

---

military threats to the country. According to the Doctrine, development of the information forces and information resistance means is one of the tasks of the Russian armed forces, alongside with the improvement of the information communication technologies across the country and in the military, the creation of basic information management systems, and integrating these systems with weapons control systems and automation and control networks.

In general, the emphasis put on information warfare in the Military Doctrine 2010 indicates that the Government of the Russian Federation assigns greater focus to cyber-warfare than to cyber-crimes. The Doctrine also informs that international cooperation is essential in the prevention of “information war”, and that Russia is dedicated to establish international partnerships in order to protect its information space.

The Law and the need for Warrants

- Article 272. Illegal access to computer information.
- Article 273. The creation, use and distribution of malicious software.
- Article 274. Misuse of means of storage, processing or transmission of computer information and telecommunications networks.

The internet has become a domestic political issue in Russia. In 2012 then-President Dmitry Medvedev (now Prime Minister) suggested to create a special cyber-police force, for the investigation of particularly technically complex crimes. This new authority is supposed to be formed as a subdivision of the national police force and is intended to replace Department “K”, but such an agency has not been formed yet.

The Minister of Internal Affairs, General Rashid Nurgaliyev, stated that one of the new areas of priority for this new agency should be to combat extremism, and that MVD was developing a legislative framework for the cyber-police to address issues of extremism on the internet. However, there are concerns over this initiative, voiced by human rights activists, that instead of investigating hacker attacks and internet fraud the cyber-police will exceed its authority and persecute ‘extremists’ who are the current government’s political opponents.

---


100 By background information, ‘Police’ (or Politsiya – “полиция” in Russian) is the new law enforcement authority in Russia; it was formed in 2011 to replace the ‘Militia’ (or Militsiya – Russian: “милиция”), which was the former civilian police authority. One of the main objectives of the reform was to improve the public image of the law enforcement authorities, and increase trust and confidence in the police.
China
Recent reports by UK and US-based private information security companies and government intelligence agencies suggest that China and Russia invest their resources in industrial espionage, and that the risks of cyber-attacks from these two countries are very high. Law firms have been identified as high-risk targets… Indeed, the international fear about the threat of cyber attacks from People’s Republic of China is growing rapidly; meanwhile, however, China also has its own internal concerns about protecting their cyberspace and fighting cyber crimes within the country.

Cyber-crime v. Cyber-warfare
Does the Distinction Exist?
Chinese laws and policies do not provide a clear distinction between cyber-crime and cyber-warfare, or clear definitions. Over the past few years, a heated discussion has been raised between academics, private organizations and the public regarding the impact of cyber-warfare in China. In 2009, the state journal People’s Tribune surveyed the public awareness of cyber-warfare. According to the survey almost 60% of respondents believed the possibility of cyber-warfare was very high.

Similar to Russia, China’s public policy documents use the terms “information” and “information security” as well as “computer security.” The terms “cyber-crime” and “cyber-attacks” are not used. Further, China’s public documents on information security and related issues mostly date back to the 1990s and early 2000s. We have not been able to uncover more recent public Chinese documents, although there have been 2011 cyber-crime amendments to the Chinese Criminal Law, with more amendments forthcoming. The emphasis of the older documents is on issues that can be classified as regular cyber-crime concerns, such as computer viruses, as well as political concerns about ensuring the stability of the Chinese party system.

Where is the Focus?
The Chinese government appears to pay more attention to cyber-crimes that involve damaging the political stability and state unity rather than other cyber-criminal behaviours, such as online...
fraud. We have not uncovered public documents that discuss cyber-warfare or cyber-attacks by foreign interests.

The Law and the need for Warrants
Several Ministries regulate cyber-crime and cyber-security in China. Among them are the Ministry of Information Industry, the Ministry of Public Security, responsible for internal security, and the Ministry of State Security, which handles external security.

In 1999 China created the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC.) CNCERT/CC operates under the administration of the Ministry of Information Industry and its main responsibilities include a national cyber security monitoring center, operation center, assessment center, and media center, and support for the government so it can meet relevant social and public responsibilities regarding cyber security.

China’s Criminal Law was amended in 1997, 2000, 2009 and 2011 to refer to cyber-crimes.\textsuperscript{106} The main provisions are as follows:

- Article 285a – Accessing [hacking] of computer systems in the areas of State affairs, national defense or sophisticated science and technology
- Article 285b – Obtaining of computer data and controlling of computer systems
- Article 285c – Provision of programs or tools used to access or control computer systems
- Article 286 – Sabotaging computer systems or data, that results in systems failure.

Chinese regulations stipulate that ISPs must record data and provide them to the authorities upon request.\textsuperscript{107} There are no clear provisions on real-time surveillance in the regulations.\textsuperscript{108}

China has not joined any of the international treaties for cyber security, although it considers itself as having standards equal or superior to the Budapest Convention standards. China has long viewed to Council of Europe Treaty as “regional”, and has called, with Russia, for the UN to play a leading role in the creation of an international governance framework for the internet and its security.

\textsuperscript{106} Yong, PI New China Criminal Legislation in the Progress of Harmonization of Criminal Legislation against Cybercrime (2011)
\textsuperscript{107} Yong, PI New China Criminal Legislation in the Progress of Harmonization of Criminal Legislation against Cybercrime (2011)
\textsuperscript{108} Yong, PI New China Criminal Legislation in the Progress of Harmonization of Criminal Legislation against Cybercrime (2011)
Summary
The table below summarizes the findings from our review of the countries above.

<table>
<thead>
<tr>
<th>#</th>
<th>Country</th>
<th>Is there a clear distinction between ‘cyber-crime’ &amp; ‘cyber-attack’ in national legal/strategic documents?</th>
<th>National focus on combatting cyber-crimes</th>
<th>National focus on securing from cyber-attacks</th>
<th>Compatibility with Canadian goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Australia</td>
<td>YES</td>
<td>X</td>
<td>X</td>
<td>Significant</td>
</tr>
<tr>
<td>2</td>
<td>New Zealand</td>
<td>YES</td>
<td>X</td>
<td>X</td>
<td>Significant</td>
</tr>
<tr>
<td>3</td>
<td>UK</td>
<td>YES</td>
<td>X</td>
<td>X</td>
<td>Significant</td>
</tr>
<tr>
<td>4</td>
<td>USA</td>
<td>YES</td>
<td>X</td>
<td>X</td>
<td>Significant</td>
</tr>
<tr>
<td>5</td>
<td>Germany</td>
<td>YES</td>
<td>X</td>
<td>X</td>
<td>Significant</td>
</tr>
<tr>
<td>6</td>
<td>France</td>
<td>YES</td>
<td>X</td>
<td>X</td>
<td>Significant</td>
</tr>
<tr>
<td>7</td>
<td>Finland</td>
<td>YES</td>
<td>X</td>
<td>X</td>
<td>Moderate</td>
</tr>
<tr>
<td>8</td>
<td>Norway</td>
<td>YES</td>
<td>X</td>
<td>X</td>
<td>Moderate</td>
</tr>
<tr>
<td>9</td>
<td>Russia</td>
<td>YES</td>
<td>X</td>
<td>X</td>
<td>Moderate</td>
</tr>
<tr>
<td>10</td>
<td>China</td>
<td>NO</td>
<td>X</td>
<td>X</td>
<td>Minimal</td>
</tr>
</tbody>
</table>

Table 1. Do countries differentiate the terms “cyber-crime” and “cyber-attack” and does it affect their cyberspace security approach: do they pose greater focus on combatting cyber crimes or on protecting from cyber attacks?

Interestingly, we have observed that most often the terms “cyber-crime” or “computer crime” are not defined, but only inferred in the laws of some countries. However, these terms, as well as the more explicit definitions of “cyber-attack” as an act distinct and more serious than a cyber-crime, can be found in the national strategic documents that usually serve as guidelines for government and sometimes the private sector.

Based on the reviewed legal documents, governments are particularly concerned with such cyber-crimes as financial fraud, child pornography and illegal access to computer data – every country reviewed in this report has introduced penalties for these offences. All of the countries covered in this report are currently drafting or discussing some changes in their legislation against cyber-crime and developing new units or agencies to address the issue of cyber-attacks.

From the reviewed policies, strategic acts and agreements, we observed a striking correlation that once a country’s government starts to differentiate cyber-attacks from cyber-crimes, the strategic focus in cyber security approach shifts from simply detecting and combating criminal offences in cyberspace locally to a more complex efforts including protecting the national infrastructure from cyber attacks, either foreign or within the country. A related shift occurs from law enforcement agencies to the military forces in many countries.
Cyber-organizations similar to NAV CANADA

Our research has not uncovered private sector, not-for-profit, cyber-organizations similar in scope and mission to the Nav Canada air traffic mission; however, a number of countries have established (New Zealand, USA, Netherlands, Korea, China) or are in the process of establishing (Australia\textsuperscript{109}, Germany\textsuperscript{110}, Finland\textsuperscript{111}) National Cyber Security Centres as \textit{governmental departments} that co-ordinate cooperation between private and public sectors, assist in defending against cyber threats and raise cyber threat awareness.

Further research and policy work must be conducted to determine the viability of the Nav Canada concept to cyber-space.

Recommendations and applicability to the Canadian approach

Canada’s Cyber Security Strategy 2010 suggests the following definition of a cyber-attack:

“\textit{Cyber-attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security.}”

According to the Canadian Strategy, cyber attacks are often inexpensive, effective, low-risk, and require only basic skills from an attacker to cause significant damage. At the same time, the document states that sophisticated cyber criminals are turning to skilled cyber attackers to conduct identity theft and financial fraud via cyberspace. Meanwhile, most of the other countries reviewed in this report classify the aforementioned offences as cyber crimes, whereas cyber attacks are considered to be only actions directed against critical national infrastructure and not against individuals or businesses that have no significant affect on a national security.

Nevertheless, even though it seems as if the Canadian Government calls any criminal offence in cyberspace a “cyber-attack”, there is still a clear classification of the types of cyber-crimes such as identity theft, money laundering and extortion, child sexual abuse, cyber espionage, and “military activities”.

A centralized Integrated Cyber Crime Fusion Centre, established by the Royal Canadian Mounted Police, is in charge of raising the ability of the Royal Canadian Mounted Police to

\textsuperscript{109} Media release from Australian Prime Minister, Julia Gillard, from 01/24/2013: \url{http://www.pm.gov.au/press-office/australian-cyber-security-centre}

\textsuperscript{110} Cyber Security Strategy for Germany – February 2011.

\textsuperscript{111} Finland’s Cyber Security Strategy 2013.
respond, using a risk-based analysis approach, to requests from the Canadian Cyber Incident Response Centre regarding cyber attacks against Government or Canada’s critical infrastructure.\(^\text{112}\) There appears, as yet, to be no international cyber-equivalent to a Nav Canada which Canada may look to emulate.

With the 2013 Canadian Government decision to abandon lawful access legislation the comparative review of other countries and their approaches is largely moot.\(^\text{113}\)

**Conclusions**

The risks of cyber threats have proliferated in recent years due to technological advances, the increase in prospective gains from committing cyber-crime, and the lower likelihood of enforcement of judicial sentences. It is close to impossible to fight cybercrime exclusively on a national level, and the lack of inter-jurisdictional and international cooperation does not facilitate governments in their objective of securing cyberspace. As critical national infrastructures are upgraded and brought online they become more vulnerable and exposed to malicious attacks, which is why securing the internet is becoming a key component of Canada’s and our partners’ national security and critical infrastructure strategy.

Not all the countries reviewed in this report have established their national strategic priorities in cyberspace and made their vision and objectives transparent and publicly available. China is notable for its obfuscation. Some of the reasons for this are inconsistencies in cyber crime legislation, incoherence and confusion about the responsibilities of the government agencies in their combat against cyber crime, unclear definition of cyber crime, undefined cyber threats and risks, and the state of ICT infrastructure development in general.

Considering the hardship in detecting cyber-crime or estimating the damage of cyber-attacks, some countries may still have some illusions about the extent of cyber risks and possible threat to the national infrastructure, businesses and individuals. However, there has certainly been an increased public perception of cyber-attacks as increasing in sophistication and scope, beginning with the cyber-attacks against Estonia and Georgia in 2007 and 2008 respectively, and continuing with the Flame and Stuxnet malware exposure in 2011 and 2012. This increased public concern, coupled with public accounts of classified cyber-attacks on businesses and corporations worldwide, has led Western governments to become more concerned with cyberspace security and to increasingly militarize their cyber-responses.

Ten years ago the discussion about international cooperation in cyberspace meant establishing laws and agreeing on common goals to protect cyberspace from the attacks of the “third parties”

\(^{112}\) Canada’s Cyber Security Strategy 2010.

(terrorist groups, activists, or any other nation that is not a signatory to an agreement between parties.) Now there is heated international discussion about the need to create a global cyber treaty much like The Treaty on the Non-Proliferation of Nuclear Weapons that will prevent cyber-powers from engaging in cyber-war and from developing technologies for cyber warfare, or at the very least will lead to development of “cyber war rules of engagement.”114

---

References


Blitz, J. (2012). *Israel, Finland and Sweden top for computer security*. News report in Financial Times from 01/30/2012. URL: [http://www.ft.com/intl/cms/s/0/e626614-4ab5-11e1-a11e-00144feabdc0.html#axzz2LmTzV3No](http://www.ft.com/intl/cms/s/0/e626614-4ab5-11e1-a11e-00144feabdc0.html#axzz2LmTzV3No). Last accessed on 02/13/2013.


Fontanka.ru: Technologies. (2012, September 18). В день Интернета МВД сообщает о росте киберпреступлений (On the Internet Day MVD reported that the number of cyber


TAdviser.ru. (2012, June 6). *Киберпреступность (Cybercrime)*. URL: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C. Last accessed on 01/18/2013.


Appendix 1. Eleven countries covered in this report (including Canada) on the world map.