CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

NATIONAL CYBER SECURITY
FRAMEWORK MANUAL

EDITED BY
ALEXANDER KLIMBURG

NATO
OTAN

This publication is supported by:

The NATO Science for Peace and Security Programme

1. PRELIMINARY CONSIDERATIONS: ON NATIONAL CYBER SECURITY

Melissa E. Hathaway, Alexander Klimburg

1.1. INTRODUCTION

What, exactly, is 'national cyber security'? There is little question that the advent of the internet is having a decisive influence on how national security is being defined. Nations are increasingly facing the twin tensions of how to expedite the economic benefits of ICT[1] and the internet-based economy while at the same time protecting intellectual property, securing critical infrastructure and providing for national security. Most nations' electronic defences have been punctured and the potential costs of these activities are considerable. More than one hundred nations have some type of governmental cyber capability and at least fifty of them have published some form of a cyber strategy defining what security means to their future national and economic security initiatives.[2] There can be little doubt, therefore, that countries have an urgent need to address cyber security on a national level. The question is how this need is being formulated and addressed.

This section provides a context for how national cyber security can be conceived. It provides an introduction, not only to the topic itself, but also to the Manual as a whole, setting the scene for the further sections to explore in depth. Accordingly, this section highlights the broad set of terms and missions being used to describe the overall cyber environment. It examines how various nations integrate their respective concepts of national security and cyber security, and proposes its own definition of what national cyber security could entail. Three conceptual tools are introduced to help focus the strategic context and debate. These are termed the 'three dimensions', the 'five mandates', and the 'five dilemmas' of national cyber security. As the reader will discover, each dimension, mandate and dilemma will play a varying role in each nation's attempt to formulate and execute a national cyber security strategy according to their specific conditions. This section, like the Manual as a whole, does not attempt to prescribe a specific set of tasks or a checklist of issues that need to be resolved. Rather, it concentrates on helping to formulate a conceptual picture of what 'national cyber security' can entail.

[1] 'Information and communications technology' used interchangeably with the term 'information technology' (IT).

[2] James A. Lewis and Katrina Timlin, Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization, (Geneva: UNIDIR, 2011), http://www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf.

1.1.1. Cyber: Converging Dependencies

The internet, together with the information communications technology (ICT) that underpins it, is a critical national resource for governments, a vital part of national infrastructures, and a key driver of socio-economic growth and development. Over the last forty years, and especially since the year 2000, governments and businesses have embraced the internet, and ICT's potential to generate income and employment, provide access to business and information, enable e-learning, and facilitate government activities. In some countries the internet contributes up to 8% of gross domestic product (GDP), and member countries of both the European Union (EU) and the G20 have established goals to increase the internet's contribution to GDP.[3] This cyber environment's value and potential is nurtured by private and public sector investments in high-speed broadband networks and affordable mobile internet access, and break-through innovations in computing power, smart power grids, cloud computing, industrial automation networks, intelligent transport systems, electronic banking, and mobile e-commerce.

The rise of the internet, and the increasing social dependence on it, did not occur overnight. The first 'internet' transmission occurred in October 1969 with a simple message between two universities. Now, 294 billion e-mail are sent per day. Internet protocols evolved during the 1970s to allow for file sharing and information exchange. Now, in one day, enough information is generated and consumed to fill 168 million DVDs. In 1983 there was a successful demonstration of the Domain Name System (DNS) that provided the foundation for the massive expansion, popularisation and commercialisation of the internet. E-commerce and the e-economy were made possible in 1985 with the introduction of top-level-domains (e.g., .mil, .com, .edu, .gov) and this growth was further fuelled in 1990 with the invention of the world wide web which facilitated user-friendly information sharing and search services. Today, nearly two-thirds of the internet-using population research products and businesses online before engaging with them offline, and most use search engines like Google, Baidu, Yahoo, and Bing to complete that research. Social networks now reach over 20% of the global population.[4] SMS traffic generates $812,000 every minute.[5]

[3] David Dean et al., 'The Connected World: The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy,' *BCG. Perspectives*, 27 January 2012.

[4] comScore, 'It's a Social World: Top 10 Need-to-Knows About Social Networking and Where It's Headed,'http://www.comscore.com/Press_Events/Presentations_Whitepapers/2011/it_is_a_social_world_top_10_need-to-knows_about_social_networking.

[5] ITU-D, The World in 2010. ICT Fact and Figures, (Geneva: ITU, 2010), http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

In 1996, the International Telecommunications Union (ITU) adopted a protocol that allowed transmission of voice communication over a variety of networks. This innovation gave way to additional technological breakthroughs like videoconferencing and collaboration over IP networks. Today, 22 million hours of television and movies are watched on Netflix and approximately 864,000 hours of video are uploaded to YouTube per day.[6] Skype has over 31 million accounts and the average Skype conversation lasts 27 minutes.[7] The mobile market has also exploded, penetrating over 85% of the global population. 15% of the population use their mobile phones to shop online and there are now more mobile phones on the planet than there are people.[8]

The internet economy has delivered economic growth at unprecedented scale, fuelled by direct and ubiquitous communications infrastructures reaching almost anyone, anywhere. At the same time, infrastructure modernisation efforts have embraced the cost savings and efficiency opportunities of ICT and the global reach of the internet. Over the past decade, businesses replaced older equipment with cheaper, faster, more ubiquitous hardware and software that can communicate with the internet. At the heart of many of these critical infrastructures is an industrial control system (ICS) that monitors processes and controls the flow of information. Its functionality is like the on or off feature of a light switch. For example, an ICS can adjust the flow of natural gas to a power generation facility, or the flow of electricity from the grid to a home. Over the last decade, industry has increased connections to and between critical infrastructures and their control system networks to reduce costs and increase efficiency of systems, sometimes at the expense of resiliency.[9]

Today, businesses around the world tender services and products through the internet to more than 2.5 billion citizens using secure protocols and electronic payments. Services range from e-government, e-banking, e-health and e-learning to next generation power grids, air traffic control and other essential services, all of which depend on a single infrastructure.[10] The economic, technological, political and social benefits of the internet are at risk, however, if it is not secure, protected and available. Therefore, the availability, integrity and resilience of this core infrastructure have emerged as national priorities for all nations.

[6] Cara Pring, '100 Social Media, Mobile and Internet Statistics for 2012 (March),' *The Social Skinny*, 21 March 2012.

[7] Statistic Brain, 'Skype Statistics,' *Statistic Brain*, 28 March 2012.

[8] Edward Coram-James and Tom Skinner, 'Most Amazing Internet Statistics 2012,' Funny Junk, http://www.funnyjunk.com/channel/science/Most+Amazing+Internet+Statistics+2012/umiNGhz.

[9] Melissa E. Hathaway, 'Leadership and Responsibility for Cybersecurity,' *Georgetown Journal of International Affairs* Special Issue (Forthcoming).

[10] Services and applications include, but are not limited to: e-mail and text messaging, voice-over-IP-based applications, streaming video and real-time video-conferencing, social networking, e-government, e-banking, e-health, e-learning, mapping, search capabilities, e-books, and IPTV over the internet.

It is anticipated that a decade from now, the internet will touch 60% of the world's population (over 5 billion citizens); will interlink more than 50 billion physical objects and devices; and will contribute at least 10% of developing nations' GDP including China, Brazil, India, Nigeria and the Russian Federation.[11] These predictions, if realised, will certainly alter politics, economics, social interaction and national security. How countries nurture and protect this infrastructure will vary. Hard choices and subtle tensions will have to be reconciled, because there are at least two competing requirements under constrained fiscal budgets: delivering economic wellbeing and meeting the security needs of the nation.

Table 2: Today and the Near Future[12]

	Today	2020
Estimated World Population	7 billion people	~8 billion people
Estimated Internet Population	2.5 billion people (35% of population is online)	~5 billion people (60% of population is online)
Total Number of Devices	12.5 billion internet connected physical objects and devices (~6 devices per person)	50 billion internet connected physical objects and devices (~10 devices per person)
ICT Contribution to the Economy	~4% of GDP on average for G20 nations	10% of worldwide GDP (and perhaps more for developing nations)

1.1.2. The Cost of Connectivity

Governments around the world are pushing for citizen access to fast, reliable, and affordable communications to meet the demand curve of the e-economy. This vision is reflected in the Organisation for Economic Co-operation and Development's (OECD) Internet Economy; Europe's Digital Agenda; the United States' National Broadband Plan, and in most ITU initiatives. A number of developing nations have grasped the importance of ICT for development. Brazil, for instance, is in the middle of a major upgrade to its broadband infrastructure.[13] Progress towards becoming

[11] Dave Evans, The Internet of Things. How the Next Evolution of the Internet Is Changing Everything, (San Jose, CA: Cisco Internet Business Solutions Group, 2011), http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

[12] Evans, *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything*.

[13] Angelica Mari, 'IT's Brazil: The National Broadband Plan' *itdecs.com*, 26 July 2011.

an advanced member of the information society is often measured in terms of lower price-points, expanded bandwidth, increased speed and better quality of service, expanded education and developed skills, increased access to content and language, and targeted applications for low-end users.[14] But is the ITU measuring the right things? Should the ITU also be measuring the attendant investments in the security of that infrastructure, connectivity and information service? For example, South Korea was ranked the most advanced nation in the ITU's information society in terms of its internet penetration, high-speed broadband connections and ICT usage; yet it was also ranked by the Internet security research firm Team Cymru as 'Asia-Pacific's leading host of peer-to-peer botnets.'[15] South Korea is not the only advanced nation to experience the challenges of connectivity. Highly-connected countries are tempting targets for criminals.[16] In fact, according to Symantec, the G20 nations harbour the majority of malicious code and infected computers. Among the top three countries are China, Germany, and the United States; of those three, the United States accounts for the highest number (23%) of all malicious computer activity.[17]

The internet is under siege and the volume, velocity, variety, and complexity of the threats to the internet and globally connected infrastructures are steadily increasing. For example, it is estimated that the G20 economies have lost 2.5 million jobs to counterfeiting and piracy, and that governments and consumers lose $125 billion annually, including losses in tax revenue.[18] Organisations everywhere are being penetrated, from small businesses to the world's largest institutions. Criminals have shown that they can harness bits and bytes with precision to deliver spam, cast phishing attacks, facilitate click-fraud and launch distributed denial of service (DDoS) attacks.[19] Attack toolkits sold in the underground economy for as little as $40 allow criminals to create new malware and assemble an entire attack plan

[14] ITU, Measuring the Information Society, (Geneva: ITU, 2011), http://www.itu.int/net/pressoffice/backgrounders/general/pdf/5.pdf. See also Melissa E. Hathaway and John E. Savage, Stewardship of Cyberspace. Duties for Internet Service Providers, (Cambridge, MA: Belfer Center for Science and International Affairs, 2012), http://belfercenter.ksg.harvard.edu/files/cyberdialogue2012_hathaway-savage.pdf.

[15] Botnet: compromised, internet-connected computers typically used for illegal activities, usually without the owner's knowledge.

[16] Reuters, 'South Korea discovers downside of high speed internet and real-name postings,' *The Guardian*, 6 December 2011.

[17] Ibid.

[18] Frontier Economics Europe, Estimating the global economic and social impacts of counterfeiting and piracy. A Report commissioned by Business Action to counterfeiting and piracy (BASCAP), (Paris: ICCWBO, 2011), http://www.iccwbo.org/Data/Documents/Bascap/Global-Impacts-Study---Full-Report.

[19] See Melissa E. Hathaway, 'Falling Prey to Cybercrime: Implications for Business and the Economy,' in *Securing Cyberspace: A New Domain for National Security*, ed. Nicholas Burns and Jonathon Price (Queenstown, MD: Aspen Institute, 2012).

without having to be a software programmer.[20] In 2011, Symantec identified over 400 million unique variants of malware that exposed and potentially exfiltrated personal, confidential, and proprietary data.[21] Many governments suffered data breaches in 2011, including Australia, Brazil, Canada, India, France, New Zealand, Russia, South Korea, Spain, Turkey, the Netherlands, the United Kingdom and the United States. Hundreds of companies have also suffered significant breaches in 2011-2012, including Citigroup, e-Harmony, Epsilon, Linked-In, the Nasdaq, Sony and Yahoo. One industry report estimates that over 175 million records were breached and another industry report estimates that it cost enterprises £79 ($125.55) per lost record,[22] excluding any fines that may have been imposed for violations of national data privacy laws.

At the same time, the pace of foreign economic collection and industrial espionage activities against major corporations and governments is also accelerating. The hyper-connectivity and relative anonymity provided by ICT lowers the risk of being caught and makes espionage straightforward and attractive to conduct. In recent testimony before the United States Congress, the Assistant Director of the Counterintelligence Division of the FBI told lawmakers that the FBI is 'investigating economic espionage cases responsible for $13 billion in losses to the US economy.'[23] Some of the cases referenced include the targeting, penetration, and compromising of companies that produce security products. In particular, certificate authorities including Comodo, DigiNotar, and RSA, fell prey to their own weak security postures, which were subsequently exploited facilitating a wave of other computer breaches.[24] Digital certificates represent a second form of identity to help enhance 'trust' for financial or other private internet transactions by confirming that something or someone is genuine.[25] These certificates have become the *de facto* credentials used for secure online communications and sensitive transactions, such as online banking or accessing corporate e-mail from a home computer.

[20] Symantec Corporation, Internet Security Threat Report: 2011 Trends, (Mountain View, CA: Symantec Corporation, 2012), http://www.symantec.com/threatreport.

[21] Ibid., 9.

[22] Verizon, 2012 Data Breach Investigations Report, (Arlington, VA: Verizon Business, 2012), http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf; Ponemon Institute, 2010 Annual Study: U.K. Cost of a Data Breach. Compliance pressures, cyber attacks targeting sensitive data drive leading IT organisations to sometimes pay more than necessary, (Mountain View, CA: Symantec Corporation, 2011), http://www.symantec.com/content/en/us/about/media/pdfs/UK_Ponemon_CODB_2010_031611.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach.

[23] U.S. House of Representatives, *Testimony: Before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, House of Representatives: Committee on Homeland Security*, 28 June 2012.

[24] Hathaway, 'Leadership and Responsibility for Cybersecurity.'

[25] Certificate Authorities issue secure socket layer (SSL) certificates that help encrypt and authenticate websites and other online services.

During oral testimony before the US Senate Armed Services Committee, US Army General Keith Alexander identified China as the prime suspect behind the RSA penetration and subsequent theft of intellectual property.[26] Perhaps the US National Counter-Intelligence Executive put it best when he reported that, '[m]any states view economic espionage as an essential tool in achieving national security and economic prosperity. Their economic espionage programs combine collection of open source information, HUMINT, signals intelligence (SIGINT), and cyber operations – to include computer network intrusions and exploitation of insider access to corporate and proprietary networks – to develop information that could give these states a competitive edge over the United States and other rivals.'[27]

Finally, unauthorised access, manipulation of data and networks, and destruction of critical resources also threatens the integrity and resilience of critical core infrastructures. The proliferation and replication of worms like Stuxnet, Flame, and Duqu that can penetrate and establish control over remote systems is alarming. In an April 2012 newsletter, the Industrial Control System Computer Emergency Readiness Team (ICS-CERT) disclosed that it was investigating attempted intrusions into what it described as 'multiple natural gas pipeline sector organisations.' It went on to say that the analysis of the malware and artefacts associated with this activity was related to a single campaign with the initial penetration, resulting from spear-phishing multiple personnel.[28] While the Stuxnet attack against Iran was quite sophisticated, it does not necessarily require a strong industrial base or a well-financed operation to find ICS vulnerabilities – teenagers regularly are able to accomplish the task.[29] Those motivated to do harm seek software vulnerabilities – effectively errors in existing software code – and create malware to exploit them, subsequently compromising the integrity, availability and confidentiality of the ICT networks and systems.[30] Some researchers hunt for these 'zero-day' vulnerabilities on behalf of governments, others on behalf of criminal syndicates, but many 'white hat' researchers constantly do the same job for little or no pay. To encourage the 'white hat' security community to effectively find holes in their commercial

[26] U.S. Senate Committee on Armed Services, *Statement of General Keith B. Alexander, Commander United States Cyber Command*, 27 March 2012.

[27] U.S. Office of the National Counterintelligence Executive, Foreign Spies Stealing US Economic Secrets in Cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011, (Washington, DC: US Office of the National Counterintelligence Executive, 2011), http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

[28] ICS-CERT, ICS-CERT Monthly Monitor, (Washington, DC: US Department of Homeland Security, 2012), http://www.us-cert.gov/control_syssupratems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf.

[29] Robert O'Harrow, 'Cyber search engine Shodan exposes industrial control systems to new risks,' *The Washington Post*, 3 June 2012.

[30] Hathaway, 'Leadership and Responsibility for Cybersecurity.'

products before criminals or cyber warriors do, companies like Google, Facebook, and Microsoft have programmes that pay for responsibly disclosed vulnerabilities.[31]

The above examples illustrate that the internet and its associated global networks have greatly increased the world's dependence on ICT and thus also increased the level of disruption that is possible when the infrastructure is under attack. And it is constantly under attack, both by state and non-state actors. Although the problem is obvious, the role of government *vis-à-vis* the private sector in the protection of this critical infrastructure is often still unclear. This lack of clarity and vision regarding government action is not totally unsurprising, however. To date, there is not even a universal understanding on basic cyber terms and definitions, so common solutions will remain scarce.

1.2. CYBER TERMS AND DEFINITIONS

The internet, the ICT that underpin it and the networks that it connects are at times also referred to as comprising 'cyberspace'. Merriam-Webster defines 'cyber' as: 'of, relating to, or involving computers or computer networks (as the Internet).'[32] Cyberspace is more than the internet, including not only hardware, software and information systems, but also people and social interaction within these networks. The ITU uses the term to describe the 'systems and services connected either directly to or indirectly to the internet, telecommunications and computer networks.'[33] The International Organisation for Standardisation (ISO) uses a slightly different term, defining cyber as 'the complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form.'[34] Separately, governments are defining what they mean by cyberspace in their national cyber security strategies (NCSS). For example, in its 2009 strategy paper, the United Kingdom refers to cyberspace as 'all forms of networked, digital activities; this includes the content of and actions conducted through digital networks.'[35] By adding the phrase, 'the content of and actions conducted through,' the government

[31] Chris Rodriguez, 'Vulnerability Bounty Hunters,' *Frost & Sullivan*, 3 February 2012.

[32] Cyber, Merriam-Webster, http://www.merriam-webster.com/dictionary/cyber.

[33] ITU, ITU National Cybersecurity Strategy Guide, (Geneva: ITU, 2011), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf. 5.

[34] ISO/IEC 27032:2012, 'Information technology – Security techniques – Guidelines for cybersecurity.'

[35] UK Cabinet Office, *Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space* (Norwich: The Stationery Office, 2009). 7. However, in 2011 a new definition of cyberspace was put forward understood as an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services (see UK Cabinet Office, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world* (London: UK Cabinet Office, 2011).).

can also address human behaviours that it finds acceptable or objectionable. For some nations, this includes consideration of internet censorship, online information control, freedom of speech and expression, respect for property, protection of individual privacy, and the protection from crime, espionage, terrorism, and warfare. Governments, businesses, and citizens know intuitively that cyberspace is man-made and an ever-expanding environment, and that therefore the definitions are also constantly changing.

1.2.1. Information, ICT, and Cyber Security

Most governments start their NCSS process by describing the importance of 'securing information', implementing 'computer security' or articulating the need for 'information assurance'. These terms are often used interchangeably, and contain common core tenets of protecting and preserving the confidentiality, integrity and availability of information. 'Information security' focuses on data regardless of the form the data may take: electronic, print or other forms. 'Computer security' usually seeks to ensure the availability and correct operation of a computer system without concern for the information stored or processed by the computer. 'Information assurance' is a superset of information security, and deals with the underlying principles of assessing what information should be protected. Effectively, all three terms are often used interchangeably, even if they address slightly different viewpoints. Most unauthorised actions that impact any of the core tenets or information security attributes[36] are considered a crime in most nations.

The globalisation of the ICT marketplace and increasing reliance upon globally sourced ICT products and services can expose systems and networks to exploitation through counterfeit, malicious or untrustworthy ICT. And while not defined in diplomatic fora, the term 'ICT security' is often used to describe this concern. In general, ICT security is more directly associated with the technical origins of computer security, and is directly related to 'information security principles' including the confidentiality, integrity and availability of information resident on a particular computer system.[37] ICT security, therefore, extends beyond devices that are connected to the internet to include computer systems that are not connected to any internet. At the same time, the use of the term 'ICT security' usually excludes all questions of illegal content, unless they directly damage the system in question, and includes the term 'supply chain security'.

[36] The most basic attributes are Confidentiality, Integrity and Availability, and are known as the C-I-A triad. Some systems expand this by including authenticity, reliability, or any number of other attributes as well.

[37] See, for instance, US DoC/NIST, Minimum Security Requirements for Federal Information and Information Systems, (Gaithersburg, MD: NIST, 2006), http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

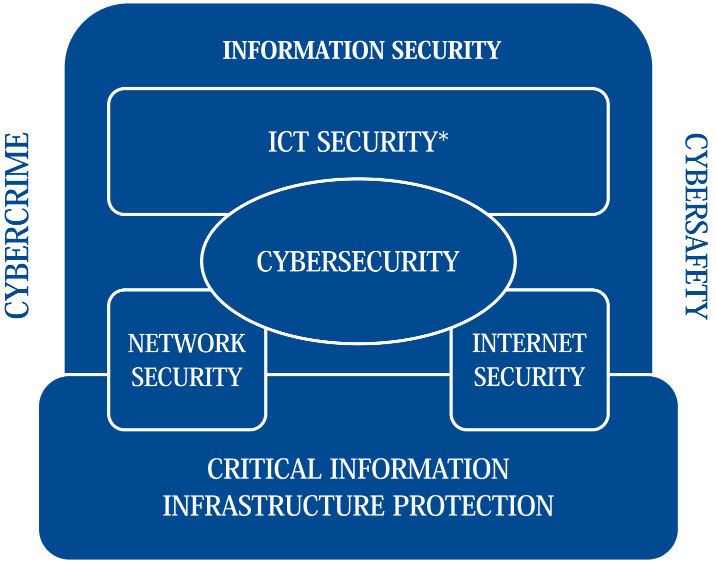

Figure 1: Relationship between Cyber Security and other Security Domains[38]

[38] This Figure has been adopted from ISO/IEC 27032:2012, 'Information technology – Security techniques – Guidelines for cybersecurity.' It slightly differs from the original in that it contains ICT Security* instead of 'Application Security'. The latter has been defined as 'a process to apply controls and measurements to an organization's applications in order to manage the risk of using them. Controls and measurements may be applied to the application itself (its processes, components, software and results), to its data (configuration data, user data, organization data), and to all technology processes and actors involved in the application's life circle' (ibid., 10.). Information Security 'is concerned with the protection of confidentiality, integrity, and availability of information in general, to serve the needs of the applicable information user' (ibid.). Network Security 'is concerned with the design, implementation, and operation of networks for achieving the purposes of information security on networks within organizations, between organizations, and between organizations and users' (ibid.). Internet Security 'is concerned with protecting internet-related services and related ICT systems and networks as an extension of network security in organizations and at home, to achieve the purpose of security. Internet Security also ensures the availability and reliability of Internet services' (ibid., 11.). CIIP 'is concerned with protecting the systems that are provided or operated by critical infrastructure providers, such as energy, telecommunication, and water departments. CIIP ensures that those systems and networks are protected and resilient against information security risks, network security risks, internet security risks, as well as Cybersecurity risks' (ibid.). Cybercrime has been defined as the 'criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime' (ibid., 4.). Cybersafety has been defined as the 'condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable' (ibid.). 'Cybersecurity', or 'Cyberspace Security' has been defined as the 'preservation of confidentiality, integrity and availability of information in the Cyberspace' (ibid.). However, it has also been noted that '[i]n addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved' (ibid.) in cyber security.

The United States, India, Russia and many other countries are increasingly voicing concerns that the introduction of counterfeit, malicious or untrustworthy ICT could disrupt the performance of sensitive national security systems, and compromise essential government services. The ICT supply chain consists of many phases, including design, manufacture, integrate, distribute, install and operate, maintain and decommission. The processes by which nations consider the security of their ICT supply chain should try to address each phase of the lifecycle. Protection measures must be developed across the product lifecycle and be reinforced through both acquisition processes and effective implementation of government/enterprise security practices. For example, the highest risk factors in the supply chain are 'after build' (e.g., during the install and operate and retire phases) because this is where multiple vendors participate in the process (e.g., integrate products with other systems, patch/update, etc.) and there are few measures to monitor and assure integrity throughout the entire process. This is a problem for all countries: the evolution of the ICT industry means that many countries and global corporations now play a role in the ICT supply chain, and no country can source all components from totally 'trusted providers'. This trust is needed, however, as the promise of ICT-driven economic growth is dependent upon the core infrastructure being both secure and resilient.

There is no agreed definition of 'internet security'. Within a technical context, internet security 'is concerned with protecting internet-related services and related ICT systems and networks as an extension of network security in organizations and at home, to achieve the purpose of security. Internet security also ensures the availability and reliability of internet services.'[39] However, in a political context, internet security is often equated with what is also known as 'internet safety'. In general, internet safety refers to 'legal internet content'. While this has sometimes been linked to government censorship in autocratic governments, restrictions on internet content are, in fact, common. Besides issues surrounding the exploitation of children, internet censorship can also include issues such as intellectual property rights as well as the prosecution of political or religious views. What internet security probably does not include is non-internet relevant technical issues, including those that address the various 'internets' which are not connected to the world wide web. These, however, are covered by the term 'network security'. Network security is particularly important for critical infrastructures that are often not directly connected to the internet. Consequently, for some, internet security implies a global government regime to deal with the stability of the internet code and hardware, as well as the agreements on the prosecution of illegal content.

[39] ISO/IEC 27032:2012, 'Information technology – Security techniques – Guidelines for cybersecurity,' 11.

The term ‘cyber security’ was widely adopted during the year 2000 with the ‘clean-up’ of the millennium software bug.[40] When the term ‘cyber security’ is used, it usually extends beyond information security and ICT security. ISO defined cyber security as the ‘preservation of confidentiality, integrity and availability of information in the Cyberspace.’[41] The Netherlands defined cyber security more broadly, to mean ‘freedom from danger or damage due to the disruption, breakdown, or misuse of ICT. The danger or damage resulting from disruption, breakdown or misuse may consist of limitations to the availability or reliability of ICT, breaches of the confidentiality of information stored on ICT media, or damage to the integrity of that information.’[42] The ITU also defined cyber security broadly as:

> ‘[T]he collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user’s assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality.’[43]

Many countries are defining what they mean by cyber security in their respective national strategy documents. As of the publication of this Manual, more than 50 nations have published some form of a cyber strategy defining what security means to their future national and economic security initiatives.

When the term ‘defence’ is paired with ‘cyber’ it usually is within a military context, but also may take into account criminal or espionage considerations. For example, the North Atlantic Treaty Organisation (NATO) uses at least two terms when it comes to cyber defence and information security. The first addresses a broader information security environment: communications and information systems[44]

[40] The millennium bug was a problem for both digital (computer-related) and non-digital documentation and data storage situations which resulted from the practice of abbreviating a four-digit year to two digits.

[41] ISO/IEC 27032:2012, ‘Information technology – Security techniques – Guidelines for cybersecurity.’

[42] Dutch Ministry of Security and Justice, ‘The National Cyber Security Strategy (NCSS). Strength through Cooperation,’ (The Hague: National Coordinator for Counterterrorism and Security, 2011), 4.

[43] Recommendation ITU-T X.1205 (04/2008), Section 3.2.5.

[44] CIS security is defined as: The ability to adequately protect the confidentiality, integrity, and availability of Communication and Information Systems (CIS) and the information processed, stored or transmitted.

(CIS) security, where 'security' is defined as the ability to adequately protect the confidentiality, integrity and availability of CIS and the information processed, stored or transmitted.[45] NATO uses a different definition for the term 'cyber defence': 'the ability to safeguard the delivery and management of services in an operational CIS in response to potential and imminent as well as actual malicious actions that originate in cyberspace.'[46] The United States military defines it in two contexts as well. The first, from the Joint Staff, defines 'computer network defence' (CND) as: 'actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks.'[47] Finally, the newly formed United States Cyber Command operationalised the term and defines 'defensive cyber operations' as: 'direct and synchronize actions to detect, analyse, counter and mitigate cyber threats and vulnerabilities; to outmanoeuvre adversaries taking or about to take offensive actions; and to otherwise protect critical missions that enable US freedom of action in cyberspace.'[48]

The common theme from all of these varying definitions, however, is that cyber security is fundamental to both protecting government secrets and enabling national defence, in addition to protecting the critical infrastructures that permeate and drive the 21st century global economy. The slight differentiation in definition between governments and intergovernment organisations is irrelevant, as their shared focus on the issues illustrates the first step in the long journey to actually providing for cyber security – no matter what the definition.

1.2.2. Cyber Crime

There does not appear to be a common view regarding what constitutes illegal or illicit activity on the internet. Yet most would agree that one of the fastest-growing areas of crime is that which is taking place in cyberspace.[49] Efforts to clarify and address this issue began in the United Nations (UN) in 1990, where the General Assembly (UN GA) debated and adopted a resolution dealing with computer crime legislation which was later expanded in 2000 and again in 2002 to combat the

[45] Geir Hallingstad and Luc Dandurand, *Cyber Defence Capability Framework – Revision 2. Reference Document RD-3060* (The Hague: NATO C3 Agency, 2010).

[46] Ibid.

[47] US Joint Chiefs of Staff, Joint Publication 6-0. Joint Communications System, (Ft. Belvoir, VA: DTIC, 2010), http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf.

[48] GAO, Defense Department Cyber Efforts. More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities, (Washington, DC: GAO, 2011), http://www.gao.gov/products/GAO-11-421. 5.

[49] Europol, Threat Assessment (Abridged). Internet Facilitated Organised Crime (iOCTA), (The Hague: Europol, 2011), https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf.

criminal misuse of ICT.[50] As a result, these early discussions encouraged countries to update their penal codes. For example, in 1997, the Russian government updated the Russian Penal Code (Chapter 28) to address cyber crime, IT crime, and cyber terrorism. Penalties were identified for, among other things, illegal access to the information on a computer, computer systems and networks; creation, spreading and usage of harmful software and malware; violation of operation instructions of a computer, computer systems and networks; illegal circulation of objects of intellectual property; illegal circulation of radio-electronic and special high-tech devices; and manufacturing and spreading of child pornography.

Also in 1997, the felonies of 'illegal intrusion into a computer information system' and 'causing damage to a computer information system' were specifically added to the Criminal Law of the People's Republic of China. In June 2010, the Information Office of the State Council published a white paper on the internet in China. It detailed China's principles for the internet and identified particular activities that were objectionable to the state. For example, it stated: 'the security of telecommunications networks and information shall be protected by law. No organization or individual may utilise telecommunication networks to engage in activities that jeopardise state security, the public interest or the legitimate rights and interests of other people.'[51] In addition to China and Russia, many other countries also have updated their legal frameworks to address criminal activities in accordance with the spirit of the discussion that began nearly 25 years ago.

The Council of Europe (CoE) also adopted a Convention on Cybercrime in July 2004,[52] the first international convention to address this issue. It contains a relatively high standard of international cooperation for investigating and prosecuting cyber crime. It recognised that criminals exploit the seams of cross-jurisdictional cooperation and coordination among nations. The treaty defined key terms such as 'computer system', 'computer data', 'traffic data', and 'service provider' in an effort to create commonality among signatories' existing statutes, but does not define the key term 'cybercrime'. The treaty went on to highlight actions that nations must undertake to prevent, investigate and prosecute, including copyright infringement, computer-related fraud, child pornography and violations of network security. For example, it outlined offences against the confidentiality, integrity and availability of computer data and systems (e.g., illegal access, illegal interception, data interference, system interference, misuse of devices). It also discussed computer-related fraud and forgery. The treaty also contained a series of powers and procedures, such as the

[50] Marco Gercke, 'Regional and International Trends in Information Society Issues,' in *HIPCAR – Working Group 1* (St. Lucia: ITU, 2010).

[51] Chinese Information Office of the State Council, *The Internet in China (White Paper)* (Beijing: Government of the People's Republic of China, 2010).

[52] Council of Europe, *Convention on Cybercrime (ETS No. 185)* (Budapest: Council of Europe, 2001).

search of computer networks and interception. Over ten years after the treaty was formed, it has been signed by 47 states, and has been ratified by 37.[53, 54] This is controversial in some nations, and might explain the relatively small number of countries that have managed to approve the treaty in accordance with their domestic constitutional requirements and thereby making it enforceable.

Other organisations have taken similar approaches, within their own frameworks. In July 2006, the ASEAN Regional Forum (ARF) issued a statement that its members should implement cyber crime and cyber security laws 'in accordance with their national conditions and should collaborate in addressing criminal and terrorist misuse of the Internet.'[55] These commitments were later codified in the 2009 agreement within the Shanghai Cooperation Organization (ASEAN-China Framework Agreement) on information security. Additionally, it is the only international treaty that addresses concerns of a wider concept of 'information war', which the treaty defined as 'confrontation between two or more states in the information space aimed at damaging information systems, processes and resources, and undermining political, economic and social systems, mass brainwashing to destabilise society and state, as well as forcing the state to take decisions in the interest of an opposing party.'[56]

Illicit and illegal activity definitions differ from region to region. Online fraud, online theft and other forms of cyber crimes which misappropriate the property of others are on the rise. It is inexpensive to develop and use malware, as was observed in 2011 with the 400 million unique variants and as many as eight new zero-day vulnerabilities were exploited per day.[57] As citizens adopt and embed more mobile devices into their business and personal lives, it is likely that malware authors will create mobile specific malware geared toward the unique opportunities that the mobile environment presents for abuse of electronic transactions and payments. Nations around the world have identified cyber crime (however it is defined) as a national priority. They also recognise that jurisdiction for prosecuting cyber crime stops at national borders, which underscores the need for cooperation and coordination through regional organisations like ASEAN and the Council of Europe.

[53] Brian Harley, 'A Global Convention on Cybercrime?,' *Science and Technology Law Review*, 23 March 2010.

[54] Council of Europe, 'Convention on Cybercrime (Treaty Status),' http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

[55] Greg Austin, 'China's Cybersecurity and Pre-emptive Cyber War,' *NewEurope*, 14 March 2011.

[56] See Shanghai Cooperation Organization, *Agreement on Cooperation in the Field of Ensuring International Information Security [based on unofficial translation]* (Yekaterinburg: Shanghai Cooperation Organization, 2009). Annex I; Nils Melzer, 'Cyber operations and *jus in bello*,' *Disarmament Forum*, no. 4 (2011).

[57] Symantec Corporation, *Internet Security Threat Report: 2011 Trends*. See also Hathaway, 'Falling Prey to Cybercrime: Implications for Business and the Economy.'

1.2.3. Cyber Espionage

Cyberspace provides an exceptional environment for espionage because it provides 'foreign collectors with relative anonymity, facilitates the transfer of a vast amount of information, and makes it more difficult for victims and governments to assign blame by masking geographic locations.'[58] While some nations define these intrusions or unauthorised access to data or an automated information system as an 'attack,' most of the observed activity today does not qualify as an attack under international law. It is considered to be theft of commercial intellectual property and proprietary information, of data with significant economic value, or the theft of government sensitive and classified information. These given considerations are defined by almost all nations as criminal acts first, and espionage second. This is also a simple necessity: with the rise of presumed state-sponsored industrial espionage, it is very often unclear if an activity that for certain can be categorised as cyber crime should instead be described as cyber espionage.

Espionage is defined as, 'the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company.'[59] In this context, espionage is when foreign governments or criminal networks steal information or counterfeit goods in ways that erode the public's trust in internet services. It is pervasive throughout the world, the number of businesses falling victim to these crimes increases daily and no sector is without compromise. Companies and governments regularly face attempts by others to gain unauthorised access through the internet to their data and information technology systems by, for example, masquerading as authorised users or through the surreptitious introduction of malicious software.[60] Some define this activity as Computer Network Exploitation (CNE): enabling operations and intelligence collection capabilities through the use of computer networks to gather data from target or adversary automated information systems or networks.[61] It is important to note that CNE is often an enabling prerequisite for disruptive or damaging activities on an information system (see below).

However it is defined, cyber espionage, particularly when targeting commercial intellectual property, risks, over time, undermining a national economy. Many countries use espionage to spur rapid economic growth based on advanced technology, targeting science and technology initiatives of other nations. Because

[58] US Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011.*

[59] Espionage, Merriam-Webster, http://www.merriam-webster.com/dictionary/espionage.

[60] See Hathaway, 'Falling Prey to Cybercrime: Implications for Business and the Economy.'

[61] U.S. Joint Chiefs of Staff, Joint Publication 3-13. Information Operations, (Ft. Belvoir, VA: DTIC, 2006), http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

ICT forms the backbone of nearly every other technology used in both civilian and military applications today, it has become one of the primary espionage targets. Of course, military and civilian dual-use technologies will remain of interest to foreign collectors, especially advanced manufacturing technologies that can boost industrial competitiveness.

1.2.4. 'Cyber Warfare'

The term 'cyber warfare' is both ambiguous and controversial – there is no official or generally accepted definition. While the term itself is virtually never used in official documents, its relatives – 'Information Operations' (Info Ops or also IO) and 'Information Warfare' (IW) – are commonly used, albeit with different meanings. More than 30 countries have an articulated doctrine and have announced dedicated offensive cyber warfare programmes, mostly using IO or IW as terminology.[62] Nonetheless, the term 'cyber war' has a useful academic purpose, in terms that it concentrates thinking on state to state conflict within and through cyberspace, and the ramifications this can have. Accordingly, cyber warfare has become an unavoidable element in any discussion of international security. For example, Russia discusses information warfare methods as a means to 'attack an adversary's centres of gravity and critical vulnerabilities,' and goes on to state that by doing so, 'it is possible to win against an opponent, militarily as well as politically, at a low cost without necessarily occupying the territory of the enemy.'[63, 64] This doctrine is a synthesis of the official position of state policy for maintaining information security. Likewise, China also discusses information warfare in depth, and the need to conduct offensive operations exploiting the vulnerabilities and dependence of nations on ICT and the internet in a recently published book.[65] China continues

[62] Lewis and Timlin, *Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization.*

[63] Roland Heickerö, Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations, (Stockholm: Swedish Defence Research Agency 2010), http://www.highseclabs.com/Corporate/foir2970.pdf. 18.

[64] Alexander Klimburg and Heli Tirmaa-Klaar, Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU, (Brussels: European Parliament, 2011), http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/EP_Study_FINAL.pdf.

[65] For a recent non-state Chinese account see Hunan People's Publishing House, *China Cyber Warfare: We Can't Lose the Cyber War* (Hunan: China South Publishing & Media Group).

to evolve its military strategy and doctrine for conducting information warfare campaigns and taking advantage of the 'informationisation'[66] of society.

Of course when nations begin to discuss cyber warfare, they need to clarify what they mean by cyber attack.[67] Germany defines a cyber attack as an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security – confidentiality, integrity and availability – which may all or individually be compromised.[68] The United Kingdom outlined four different methods of cyber attack in its national cyber strategy: electronic attack, subversion of supply chain, manipulation of radio spectrum, disruption of unprotected electronics using high power radio frequency.[69] The United States defines Computer Network Attack (CNA) as 'actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves'.[70] The difference between the US and German definition of cyber attack is an illustrative one: the US definition does not include attacks on confidentiality (e.g., through a 'probe' or espionage) as a cyber attack while, according to the German definition, there is no difference between a probe and a cyber attack. The term takes on different meanings to meet the security remit of different communities. For example, it is natural for the military to be ambiguous as to whether an attack is considered a use of force (as defined by the Law of Armed Conflict), whereas the law enforcement community (police and prosecutors) are more likely to describe an attack as a crime. Incident response professional and technical experts will likely use the term to generically characterise any malicious attempt against confidentiality or availability. A single definition will not help this, but clarity about which meaning of 'attack' is meant in a particular context can help reduce confusion.

In general, there is agreement that cyber activities can be a legitimate military activity, but there is no global agreement on the rules that should apply to it. This is further complicated by the ambiguous relationship between cyber war and cyber

[66] China has is promoting informationisation development for economic restructuring, infrastructure modernisation, and national security. It is similar to the Digital Agenda of Europe, in that it is promoting all the means to accelerate the process from the industry society to the information society. It contains seven areas of emphasis: (1) ICT and ICT industries (manufacture, service); (2) ICT applications (e-gov, e-commerce); (3) Information Resources (Content); (4) Information Infrastructure (Network); (5) Information Security; (6) Talents (all kinds); (7) Laws, Regulations, Standards, and Specifications (see Xiaofan Zhao, 'Practice and Strategy of Informatization in China,' (Shanghai: UPAN, 2006).).

[67] See Section 3.1.3 for a more detailed examination of cyber attack classifications.

[68] German Federal Ministry of the Interior, *Cyber Security Strategy for Germany* (Berlin: Beauftragter der Bundesregierung für Informationstechnik, 2011). 14-5.

[69] UK Cabinet Office, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*: 13-4.

[70] U.S. Joint Chiefs of Staff, *Joint Publication 3-13. Information Operations*.

espionage – there is a very fine line between breaking into a computer to spy and breaking in to attack.[71] Nations are concerned that infrastructure disruption could inflict significant economic costs on the public and private sectors and impair performance of essential services. This is why some nations are demanding a dialogue regarding what constitutes a legitimate target in cyberspace, code of conduct for stewardship and conflict, and the need for confidence building measures to reduce the risk of unwanted or unnecessary miscalculation and subsequent escalation of conflict and misunderstanding.

For example, China, Russia, Tajikistan and Uzbekistan introduced an International Code of Conduct for Information Security for consideration by the 66th UN General Assembly.[72] This document was intended to jumpstart discussion on wide-ranging approaches for dealing with appropriate behaviours in cyberspace. This specific proposal and the overall concept of a 'code of conduct', will likely be raised at a number of upcoming international fora dealing with cyber security and internet policy matters.

To date, it appears that the United States and a number of European countries oppose the notion that a code of conduct or treaty is needed to address cyber warfare. They argue that the proposed obligations seem to be in conflict with existing international law built around concepts such as refraining from the 'threat or use of force' (Article 2(4) of the UN Charter) and the right to exercise 'self-defence if an armed attack occurs' (Article 51 of the UN Charter). Moreover, it is unclear how a proposed code's concepts of 'hostile activities' and 'threats to international peace and security' relate to the 'threat or use of force' standard in Article 2(4), or whether the proposed code would constrain the inherent right to self-defence recognised in Article 51. Other nations are taking the initiative to drive debate and resolution regarding what is needed, given the economic and national security consequences of what is at stake. These efforts have taken on a new tempo and seriousness given the use of Stuxnet against Iran's nuclear infrastructure. For example, the United Kingdom hosted a conference on norms of behaviour in London in 2011 to help foster an international dialogue, and it is expected that this discussion will continue in Hungary and South Korea in the coming years.

[71] James Lewis, 'Confidence-building and international agreement in cybersecurity,' *Disarmament Forum*, no. 4 (2011): 56.

[72] See UNGA, *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359)* (New York: United Nations, 2011).

1.3. NATIONAL CYBER SECURITY

There is no universally accepted explicit definition of what constitutes 'national cyber security' (or NCS for short). Indeed, although the exact term is hardly ever used in official strategies, it is commonly employed by government spokespersons without ever being defined. NCS has two obvious roots: the term 'cyber security' and the term 'national security' – both of which are often differently defined in official national documents. Even if the term 'national cyber security' is seldom explicitly defined, it is possible to derive a working definition based on the respective use of the other two terms.

1.3.1. Comparison of 'National' and 'Cyber' Security

When analysing the use of the terms 'cyber security' and 'national security' in official documents, it is first and foremost necessary to accept that national differences (to say nothing of linguistic differences) will often prevent a direct and literal comparison. As discussed above, the term 'cyber security' does not have a single accepted common definition, and this is especially the case when used within public policy documents. Also, the term 'national security' is not always defined even within a specific national context – an often intentional move aimed to provide government with needed flexibility.[73]

Until relatively recently, the term 'national security' was largely used only within the United States. The widespread introduction of dedicated 'national security strategies' (NSS) in a number of OECD countries is a relatively recent phenomenon that appears to have been closely tied to a shift in strategic thought away from focusing on a few specific 'threats' to the idea against of mitigation against myriad 'risks'. Thus, for example, in nearly all of the post-2007 strategies, cyber security is defined as a key national security issue. Indeed, in some cases, the topic of 'cyber security' (or even 'national cyber security') predates the actual creation of the national security strategy, and sometimes even seems to function as a driver for the paradigm shift to a more comprehensive national security strategy; one in which the state not only recognises that various risks need to be addressed, but that they only can be addressed by working together with non-state actors.

[73] For example, the UK Security Service (also known as MI5) states that: 'The term 'national security' is not specifically defined by UK or European law. It has been the policy of successive Governments and the practice of Parliament not to define the term, in order to retain the flexibility necessary to ensure that the use of the term can adapt to changing circumstances' (UK Security Service (MI5), 'Protecting National Security,' https://www.mi5.gov.uk/home/about-us/what-we-do/protecting-national-security.html.).

When looking at specific countries, this paradigm shift becomes fairly clear. Australia, for instance, published its First National Security Statement to its Parliament in 2008,[74] which was put in place as part of a long-term reform agenda to establish a sustainable national security policy framework. When the Australian government released its Cyber Security Strategy[75] in 2009, it was clear that the strategy dealt with both Australia's national security and its digital economy. While the National Security Strategy highlights the vitality of 'partnerships between industry, governments and the community',[76] in order to maintain 'a secure, resilient and trusted electronic operating environment',[77] the government's cyber security policy has a similar emphasis on partnerships with the private sector; while simultaneously referring to the fact that 'the Australian Government has an important leadership role'.[78]

Although the term 'national security' has been used in Canada since the 1970s, the first official incorporation of a national security strategy did not occur until 2004.[79] However, as set out in its National Security Strategy, threats that 'undermine the security of the state of society [...] generally require a national response, as they are beyond the capacity of individuals, communities or provinces to address alone.'[80] In context with Canada's cyber security strategy, this implies 'a shared responsibility, one in which Canadians, their governments, the private sector and our international partners all have a role to play.'[81]

In Germany, at least until 2008, the term '*Sicherheitspolitik*' was considered to be sufficiently analogous to the English term 'national security'. But in recent years the term 'national security' has taken root in German policy and political discourse, perhaps in an effort to draw attention to the increased blurring of national and international risks (as opposed to the threat-based model of the Cold War) requiring an increased 'national' cooperation. As part of these efforts, the term 'cyber security' might be considered directly analogous to 'national cyber security', in that it is also directly tied with a single specific programme – the national protection plan for the critical information infrastructure.[82]

[74] Australian Prime Minister, *The First National Security Statement to the Australian Parliament* (Canberra: Australian Government, 2008).

[75] Australian Attorney-General's Department, *Cyber Security Strategy* (Canberra: Australian Government, 2009).

[76] Ibid., 5.

[77] Ibid.

[78] Ibid.

[79] Canadian Privy Council Office, *Securing an Open Society: Canada's National Security Policy* (Ottawa: Canadian Government, 2004).

[80] Ibid., vii.

[81] Canadian Department for Public Safety, *Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada* (Ottawa: Canadian Government, 2010). 17.

[82] The implementation of this protection plan is known as UP-KRITIS (civilian) and UP-BUND (for government).

Similarly, in France there was no formal tradition of the term 'national security' until 2008, when it was first introduced in the Defence White Book.[83] In contrast to Germany, the concept of national security was comprehensively defined, based upon both 'defence' (military) and 'domestic' (internal) civilian strategies, together with an overall set of guiding principles.[84] Recent French government documents[85] make it clear that 'cyber defence' aims to protect the security of France's 'critical information systems' according to 'information assurance measures'.

The first British National Security Strategy was introduced in 2008 and has been reviewed at least two times since. The rationale for moving away from the previous emphasis on Strategic Defence Reviews or Defence White Papers was made quite clear:

> 'The aim of this first National Security Strategy is to set out how we will address and manage this diverse though interconnected set of security challenges and underlying drivers, both immediately and in the longer term, to safeguard the nation, its citizens, our prosperity and our way of life.'[86]

The focus on this 'diverse set of security challenges' was particularly directed at cyber security. To enjoy freedom and prosperity in cyberspace, the government set out four guiding objectives: successful handling of cyber crime; establishing the UK as one of the most secure places in the world to do business; improvement of resilience to cyber attacks, and protection of national interests in cyberspace.[87] The British National Cyber Strategy is a comprehensive document that goes beyond national security issues. Although the 'national security' component of the Cyber Security Strategy remains partially classified, it appears to be well funded in that over £650 million was made available for the period 2011-2015. Interestingly, the definition of cyber security seems equally concerned with protecting systems as well as 'exploiting opportunities' and encompasses missions as diverse as internet governance, trade policy, counter-terrorism and intelligence.

[83] French White Paper Commission, *The French White Paper on Defence and National Security* (Paris: Odile Jacob, 2008).

[84] 'The 'republican compact' that binds all French people to the State, namely the principles of democracy, and in particular individual and collective freedoms, respect for human dignity, solidarity and justice' (ibid., 58.).

[85] French Secretariat-General for National Defence and Security, *Information systems defence and security. France's strategy* (Paris: French Network and Information Security Agency, 2011).

[86] UK Cabinet Office, *The National Security Strategy of the United Kingdom. Security in an interdependent world* (Norwich: The Stationery Office, 2008).

[87] UK Cabinet Office, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*: 21.

Table 3: National (Cyber) Security Strategies in Selected OECD Countries

	NATIONAL SECURITY			CYBER SECURITY			NATIONAL CYBER SECURITY
	Document	**Year**	**Basic Definition / Understanding**	**Document**	**Year**	**Basic Definition / Understanding**	**Key Objectives / Areas**
AU	The First National Security Statement to the Parliament[88]	2008	'Freedom from attack or the threat of attack; the maintenance of our territorial integrity; the maintenance of our political sovereignty; the preservation of our hard won freedoms; and the maintenance of our fundamental capacity to advance economic prosperity for all Australians.'	Cyber Security Strategy[89]	2009	'Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.'	Three key objectives: - 'All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online' - 'Australian Businesses operate secure and resilient informations and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers' - 'The Australian Government ensures its information and communications technologies are secure and resilient'
CA	Securing an Open Society: Canada's National Security Policy[90]	2004	'National security deals with threats that have the potential to undermine the security of the state or society. These threats generally require a national response, as they are beyond the capacity of individuals, communities or provinces to address alone. National security is closely linked to both personal and international security. While most criminal offences, for example, may threaten personal security, they do not generally have the same capacity to undermine the security of the state or society as do activities such as terrorism or some forms of organized crime. Given the international nature of many of the threats affecting Canadians, national security also intersects with international security. At the same time, there are a growing number of international security threats that impact directly on Canadian security and are addressed in this strategy.'	Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada[91]	2010	'detect, identify and recover' from cyber attacks which '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.'	Three pillars: - 'Securing Government systems' - 'Partnering to secure vital cyber systems outside the federal Government' - 'Helping the Canadians to be secure online'

[88] Australian Prime Minister, *The First National Security Statement to the Australian Parliament.*

[89] Australian Attorney-General's Department, *Cyber Security Strategy.*

[90] Canadian Privy Council Office, *Securing an Open Society: Canada's National Security Policy.*

[91] Canadian Department for Public Safety, Canada's Cyber Security Strategy. *For a Stronger and More Prosperous Canada.*

[92] Federal Ministry of Defence, *White Paper 2006 on German Security Policy and the Future of the Bundeswehr* (Berlin: Federal Ministry of Defence, 2006).

[93] German Federal Ministry of the Interior, *Cyber Security Strategy for Germany.*

[94] French White Paper Commission, *The French White Paper on Defence and National Security.*

[95] French Secretariat-General for National Defence and Security, *Information systems defence and security. France's strategy.*

[96] Dutch Government, *Strategie Nationale Veiligheid* (The Hague: Ministry of the Interior and Kingdom Relations, 2007).

[97] Dutch Ministry of Security and Justice, 'The National Cyber Security Strategy (NCSS). Strength through Cooperation.'

[98] UK Cabinet Office, *The National Security Strategy: A Strong Britain in an Age of Uncertainty* (Norwich: The Stationary Office, 2010).

[99] UK Cabinet Office, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.*

[100] White House, *National Security Strategy* (Washington, DC: White House, 2010).

[101] White House, *The National Strategy to Secure Cyberspace.*

[102] *National Security Presidential Directive 54: Cyber Security and Monitoring (NSPD-54) / Homeland Security Presidential Directive 23: Cyber Security and Monitoring (HSPD-23).*

[103] Public Safety and Homeland Security Bureau, 'Tech Topic 20: Cyber Security and Communications,' FCC, http://transition.fcc.gov/pshs/techtopics/techtopics20.html.

DE	White Paper 2006 on German Security Policy and the Future of the Bundeswehr[92]	2006	‘German security policy is based on a comprehensive concept of security; it is forward-looking and multilateral. Security cannot be guaranteed by the efforts of any one nation or by armed forces alone. Instead, it requires an all-encompassing approach that can only be developed in networked security structures.’	Cyber Security Strategy for Germany[93]	2011	‘Cyber security and civilian and military cyber security: (Global) cyber security is the desired objective of the IT security situation, in which the risks of global cyberspace have been reduced to an acceptable minimum. Hence, cyber security in Germany is the desired objective of the IT security situation, in which the risks of the German cyberspace have been reduced to an acceptable minimum. Cyber security (in Germany) is the sum of suitable and appropriate measures. Civilian cyber security focuses on all IT systems for civilian use in German cyberspace. Military cyber security focuses on all IT systems for military use in German cyberspace.’	Ten strategic areas (objectives and measures): - ‘Protection of critical information infrastructures’ - ‘Secure IT systems in Germany’ - ‘Strengthening IT security in the public administration’ - ‘National Cyber Response Centre’ - ‘National Cyber Security Council’	- ‘Effective crime control also in cyberspace’ - ‘Effective coordinated action to ensure cyber security in Europe and worldwide’ - ‘Use of reliable and trustworthy information technology’ - ‘Personnel development in federal authorities’ - ‘Tools to respond to cyber attacks’
FR	The French White Paper on Defence and National Security[94]	2008	‘The aim of France’s National Security strategy is to ward off risks or threats liable to harm the life of the nation. Its first aim is to defend the population and French territory, this being the first duty and responsibility of the State. The second aim is to enable France to contribute to European and international security: this corresponds both to its own security needs, which also extend beyond its frontiers, and to the responsibilities shouldered by France within the framework of the United Nations and the alliances and treaties which it has signed. The third aim is to defend the values of the ‘republican compact’ that binds all French people to the State, namely the principles of democracy, and in particular individual and collective freedoms, respect for human dignity, solidarity and justice.’	Information systems defence and security: France’s strategy[95]	2011	‘The desired state of an information system in which it can resist events from cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible. Cybersecurity makes use of information systems security techniques and is based on fighting cybercrime and establishing cyberdefence.’	Four strategic objectives: ‘- Become a cyberdefence world power in cyberdefence - Safeguard France’s ability to make decisions through the protection of information related to its sovereignty - Strengthen the cybersecurity of critical national infrastructures - Ensure security in cyberspace’	
NL	Strategie Nationale Veiligheid[96]	2007	[*Own Translation*] ‘National security is at stake when the vital interests of our state and/or our society [1. territorial security, 2. economic security, 3. ecological security, 4. physical security, and 5. social and political security] are threatened in such way that it leads to – potential – social disruption. National security contains both the corrosion of security by intentional human action (security) as well as the damage caused by disasters, system or process failures, human error or natural anomalies such as extreme weather (safety).’	The National Cyber Security Strategy (NCSS): Strength through cooperation[97]	2011	‘Cyber security is freedom from danger or damage due to the disruption, breakdown, or misuse of ICT. The danger or damage resulting from disruption, breakdown, or misuse may consist of limitations to the availability or reliability of ICT, breaches of the confidentiality of information stored on ICT media, or damage to the integrity of that information.’	‘Security and trust in an open and free digital society: The Strategy’s goal is to strengthen the security of digital society in order to give individuals, businesses, and public bodies more confidence in the use of ICT. To this end, the responsible public bodies will work more effectively with other parties to ensure the safety and reliability of an open and free digital society. This will stimulate the economy and increase prosperity and well-being. It will ensure legal protection in the digital domain, prevent social disruption, and lead to appropriate action if things go wrong.’	

UK	A Strong Britain in an Age of Uncertainty: The National Security Strategy[98]	2010	‘The security of our nation is the first duty of government. It is the foundation of our freedom and our prosperity.’ [...] ‘The National Security Strategy of the United Kingdom is: to use all our national capabilities to build Britain’s prosperity, extend our nation’s influence in the world and strengthen our security.’	The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world[99]	2011	actions taken ‘to reduce the risk and secure the benefits of a trusted digital environment for businesses and individuals.’	Four objectives: ‘- The UK to tackle cybercrime and be one of the most secure places in the world to do business in cyberspace - The UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace - The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societie - The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives’
US	National Security Strategy[100]	2010	‘Our national security depends upon America’s ability to leverage our unique national attributes, just as global security depends upon strong and responsible American leadership. That includes our military might, economic competitiveness, moral leadership, global engagement, and efforts to shape an international system that serves the mutual interests of nations and peoples. For the world has changed at an extraordinary pace, and the United States must adapt to advance ou interests and sustain our leadership.’	The National Strategy to Secure Cyberspace[101]	2003	‘protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States. We must act to reduce our vulnerabilities to these threats before they can be exploited to damage the cyber systems supporting our Nation’s critical infrastructures and ensure that such disruptions of cyberspace are infrequent, of minimal duration, manageable, and cause the least damage possible. Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from our entire society – the federal government, state and local governments, the private sector, and the American people.’	Three Strategic Objectives: ‘- Prevent cyber attacks against America’s critical infrastructures - Reduce national vulnerability to cyber attacks; and - Minimize damage and recovery time from cyber attacks that do occur.’
				National Security Presidential Directive 4[102] (partially unclassified)[103]	2008	[*From the 2009 Cyberspace Policy Review*] ‘cybersecurity policy [...] includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. The scope does not include other information and communications policy unrelated to national security or securing the infrastructure.’	[*From the 2008 National Security Presidential Directive 54*] Thirteen Objectives: ‘- establishing the National Cyber Security Center within the Department of Homeland Security’ ‘- Move towards managing a single federal enterprise network; - Deploy intrinsic detection systems; - Develop and deploy intrusion prevention tools; - Review and potentially redirect research and funding; - Connect current government cyber operations centers; - Develop a government-wide cyber intelligence plan; - Increase the security of classified networks; - Expand cyber education; - Define enduring leap-ahead technologies; - Define enduring deterrent technologies and programs; - Develop multi-pronged approaches to supply chain risk management; and - Define the role of cyber security in private sector domains.’
				Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure	2009		

The Netherlands was one of the first countries to move away from a threat-based national security picture to a more 'risk' based view.[104] As part of this shift, the first Dutch National Security Strategy was adopted in 2007, with a detailed work plan leading to the eventual adoption of a national cyber security strategy in 2011. The drafting of the strategy was coordinated by the Ministry of Security and Justice, and was a response to the Parliament's demand (referred to as the Amendment Knops) for the creation of a 'National Cyber Strategy'. The document was conceived as providing a road-map to a Whole of Government approach to national security.[105] The definition of national security is closely aligned to the philosophy of 'Comprehensive Security'[106] and initiated a national risk assessment based approach to decision making.[107] The language within the NCSS is clearly orientated toward 'ICT-based threats', and the Dutch definition of cyber security contemplates the 'freedom from danger or damage due to the disruption, breakdown, or misuse of ICT.'

The United States has used the term 'national security' at least since 1947, and in the ensuing six decades, the implicit meaning of 'national security' has changed many times – an explicit meaning was often avoided in order to secure an advantage through strategic ambiguity.[108] Since 1986, the United States has produced 15 National Security Strategies (NSS), the most recent of which was published in 2012. The US definition of 'national security' is much wider than commonly employed abroad. While 'securing cyberspace' is also a particular item within the NSS 2010, the majority of mentions of 'cyber' are outside of that particular section, illustrating that the issue is considered to be cross-vertical and not, in the most narrow sense, a security issue alone. Similarly, the US has avoided creating a dedicated single overarching national cyber security strategy, instead relying on a collection of documents to fulfil the same goal. Since the White House first established formal

[104] For an in-depth study, see Michel Rademaker, 'National Security Strategy of the Netherlands: An Innovative Approach, '*Information and Security* 23, no. 1 (2008), http://infosec.procon.bg/v23/Rademaker.pdf.

[105] See, for instance, Marcel de Haas, From Defence Doctrine to National Security Strategy: The Case of the Netherlands, (The Hague: Netherlands Institute of International Relations Clingendael, 2007), http://www.clingendael.nl/publications/2007/20071100_cscp_art_srsa_haas.pdf.

[106] The five securities are *Territorial*, *Economic*, *Physical*, *Ecological* and *Social/ Political*.

[107] Dutch Ministry of Security and Justice, 'The National Cyber Security Strategy (NCSS). Strength through Cooperation.'

[108] According to a US defence department manual, 'national security' is '[a] collective term encompassing both national defence and foreign relations of the United States. Specifically, the condition provided by: a. a military or defence advantage over any foreign nation or group of nations; b. a favourable foreign relations position; or c. a defence posture capable of successfully resisting hostile or destructive action from within or without, overt or covert' (U.S. Joint Chiefs of Staff, Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms, (Ft. Belvoir, VA: DTIC, 2012), http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.).

structures in 1998 to coordinate various cyber security activities,[109] a number of documents have been released that can claim to directly address strategic national cyber security issues.[110] Yet there is no clear definition of what the US government considers to be cyber security, although the term 'national cyber security' (albeit undefined) has been employed.[111]

1.3.2. Cyber Power and National Security

Until fairly recently there have been few theoretical models of interstate conflict and international relations that directly have cyber security at their core. The concept of 'cyber warfare' is highly contentious, not the least because, for liberal democratic governments, the distinction between warfare and mere attacks is a vital one. Not all approaches, however, make the distinction between peacetime and wartime activities. The purported Chinese 'Information Warfare'[112] concept (known as 'Three Warfares') includes methods such as 'Legal Warfare' and 'Media Warfare' that might seem to be anathema to liberal democracies, yet certainly acknowledges the importance of information in the so-called Information Age. While some nations cannot easily countenance such strategies, it is clear that a new conflict paradigm is necessary, one that acknowledges the importance of the information domain while not violating hallowed principles of democracy. An equally important question is how to include the breadth of national cyber security issues and functions in times of both peace and war, and across the different components of 'national power',[113] e.g., to exert 'cyber power'.

[109] The Critical Infrastructure Protection (PDD-63) as part of: *National Security Presidential Directive 54: Cyber Security and Monitoring (NSPD-54) / Homeland Security Presidential Directive 23: Cyber Security and Monitoring (HSPD-23)*.

[110] These include: White House, *The National Strategy to Secure Cyberspace* (Washington, DC: White House, 2003); *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7)*; White House, *The Comprehensive National Cybersecurity Initiative (as codified in NSPD-54/HSPD-23)* (Washington, DC: White House, 2008); White House, *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: White House, 2009); White House, *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World* (Washington, DC 2011).

[111] The context is a Whole of Government Cyber Security Strategy and, in particular, enhanced cooperation between the Department of Homeland Security and the Department of Defense. Overall, the term 'national cyber security' implies here the protection of the .mil and .gov domain, and the ability of the systems within these domains to operate normally at home and abroad (US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC 2011). 8.).

[112] For a comprehensive study of the 'Three Warfares Study' see Timothy Walton, 'Treble Spyglass, Treble Spear?: China's Three Warfares,' *Defense Concepts* 4, no. 4 (2009).

[113] Concepts of 'national power' refer to leverages of power of a nation-state or alliance; and can include different specific instruments. Most commonly these are referred to as including Diplomatic, Military, Informational and Economic (DIME) instruments. These are active in times of peace and war.

What actually constitutes power in and through cyberspace within the larger framework of national power is still poorly understood and the subject of much debate. What is clear is that the 'cyber power' of a nation does not necessarily derive solely from the amount of trained hackers it has, but rather the sum total of resources or capabilities it can leverage to pursue political and economic goals while ensuring the resilience of its own infrastructure.

One attempt to define cyber power reads: 'the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power.'[114] This definition illustrates what has become official policy not only in the United States, but also in many countries in Europe: cyberspace is viewed as an operational domain of military operations, equal to land, air, sea and space.[115] Unlike the other domains of conflict, however, cyberspace plays a role across each of the 'instruments of national power'. Each of these instruments is therefore directly influenced by cyber means.[116]

This approach to cyber security and national power has one particular disadvantage – it is very much a 'major power' doctrine, most applicable to nations whose size or intent propels them to seek a highly proactive engagement in the international strategic landscapes, i.e., to actively 'create strategic opportunities via cyberspace'. The discourse has largely emerged from the military, despite other attempts to define cyber power within a 'soft power' context.[117] Not all nations will share these goals of power projection.

The concept of 'national cyber security' that is seemingly emerging by default, rather than by intent, addresses a more modest set of requirements than notions of cyber power. While military capabilities and international power-projection still play a role, the view is often more orientated towards managing the cyber risks that a nation faces, rather than proactively trying to exploit those cyber risks in advancing its global power. Nations that seek to define a pronounced NCSS often do so more with a view towards domestic security, rather than expanding their global

[114] Franklin D. Kramer, Stuart H. Starr, and Larry Wentz, eds., *Cyber Power and National Security* (Washington, DC: National Defence UP, 2009).Kramer and his colleagues, however, approach the issue primarily from a military perspective. A slightly broader view was offered by Joseph Nye, who considers the most important application of soft (cyber) power to be outward-facing, influencing nations, rather than inward-facing (see Joseph S. Nye, Cyber Power, (Cambridge, MA: Belfer Center for Science and International Affairs, 2010), http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.).
See Mark Thompson, 'U.S. Cyberwar Strategy: The Pentagon Plans to Attack,' *Time*, 2 February 2010.

[115] See, for instance, US Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*.

[116] Kramer, Starr, and Wentz, *Cyber Power and National Security.*

[117] Nye, *Cyber Power*; Alexander Klimburg, 'The Whole of Nation in Cyberpower,' *Georgetown Journal of International Affairs* Special Issue (2011).

strategic position. Accordingly, for the purposes of this Manual, we will define 'national cyber security' as:

> 'the focused application of specific governmental levers and information assurance principles to public, private and relevant international ICT systems, and their associated content, where these systems directly pertain to national security.'

1.4. CONCEPTUALISING NATIONAL CYBER SECURITY

As discussed above, what ultimately constitutes national cyber security (NCS) will always remain in the eye of the beholder. However, any overall strategy that seeks to address NCS will most likely need to orientate itself according to various parameters: what is the purpose of the strategy? who is the intended audience? These questions will be addressed in full in Section 2 as they are standard questions for any national security strategy, and are independent of the cyber security domain. What is inherent to the cyber security topic are more specific questions: firstly, where is the strategy directed at, what is its actual purpose, who are the stakeholders? This question is addressed in more depth in Section 3. Secondly, how is the cyber security domain segmented, and how are the different interpretations of NCS understood? This question is addressed in more depth in Section 4. And thirdly, how does this all relate to the wider well-being of the nation?

For these last three questions this Manual suggests three conceptual tools to help focus strategic deliberations: respectively, they are termed the 'three dimensions', the 'five mandates', and the 'five dilemmas' of national cyber security. Together they provide for a comprehensive view of the topic. Not all NCSS will want to provide equal weight to the different aspects of national cyber security described in this Manual. Therefore, these tools are intended to provide an overview of what aspects can be considered, rather than a checklist of what should be taken into account.

1.4.1. The Three Dimensions: Governmental, National and International[118]

Any approach to a NCS strategy needs to consider the 'three dimensions' of activity: the governmental, the national (or societal) and the international. Since the 1990s a particular trend in public policy theory has focused on the cooperation of different

[118] See Section 3 for further details. Based on Klimburg, 'The Whole of Nation in Cyberpower.'

actors. Initially the focus was on improving the coordination of government actors (the Whole of Government approach or WoG), particularly between the departments most involved in stabilisation or peace building operations in places like Afghanistan or Iraq. Subsequently, the general notion was picked up by international organisations as diverse as NATO and the International Committee of the Red Cross, who backed concepts of international, trans-border and 'like for like' collaboration (also called the Whole of System approach or WoS) rather than intergovernmental cooperation. More recently, states have begun looking at better methods for cooperating with their 'national' non-state actors, ranging from aid and humanitarian groups to critical infrastructure providers (sometimes called the Whole of Nation approach or WoN) or even, more generally, their national civil society.

The lessons learned from the prolonged engagements in countries like Afghanistan and Iraq emphasise the importance and the challenge of different actors working together. The same challenges apply even more so to the field of national cyber security where, if anything, power and responsibility is distributed far more widely than within so-called stabilisation or peace building operations.

Governmental: within government alone, it is not unusual for up to a dozen different departments and agencies to claim responsibility for national cyber security in various forms, including military, law enforcement, judicial, commerce, infrastructure, interior, intelligence, telecommunications, and other governmental bodies. This is understandable due to breadth and depth of what constitutes NCS but leads to considerable difficulty in establishing coherent action. A major challenge for all NCS strategies is, therefore, improving the coordination between these governmental actors. This Whole of Government effort can be achieved by a number of different methods, ranging from appointing a lead agency or department to simply improving the inter-departmental process. Due to the esoteric nature of cyber security, however, it probably requires much more effort to achieve this Whole of Government synergy than practically any other security challenge.

International: virtually no NCS document ignores the international dimension. The very basis of the internet,[119] to say nothing of the myriad companies and organisations that effectively constitute the internet, is thoroughly globalised. For any nation state or interest group, to advance its interests requires collaboration with a wide range of international partners. This applies at any level: from internationally binding treaties (e.g., the Council of Europe Cybercrime Convention), to politically binding agreements (e.g., regarding Confidence Building Measures

[119] The internet is marked by the routing of data 'packets' and these packets rarely take the most direct geographic route: it is perfectly possible for an e-mail sent from Los Angeles to New York to be routed through China and Russia on the way.

in Cyberspace), to non-governmental agreements between technical certification bodies (e.g., membership of FIRST[120] and similar bodies). Many of the international collaborations will occur outside a specific national government. In fact, it can be necessary to work with non-state actors abroad. Therefore, the emphasis must be on relationships with all the relevant actors within specific systems (in particular, but not limited to the field of 'internet governance'). This Whole of System approach, therefore, emphasises the need for a government to agree on a single lead actor (which can be also outside of government itself), and to enable that actor to be flexible enough to engage with the entire range of actors globally.[121]

National: engagement with security contractors and critical infrastructure companies has always been seen as critical for national security. The steady expansion of the number of actors relevant to national cyber security within any particular nation has meant that some governments have decided to make their overall strategy 'comprehensive', including the entire society, or the Whole of Nation. A Whole of Nation approach tries to overcome the limitations of simply having special legally-defined relationships with a small number of specific security contractors. Often it tries to encourage a wide range of non-state actors (in particular private companies but also research establishments and civil society) to cooperate with the government on cyber security issues. While many governments are increasingly expanding their legal options, the general principle is that specific 'cooperation' is needed from such a great number of non-state actors that a pure legislative approach would be largely unworkable in most democracies. To encourage cooperation, Whole of Nation approaches usually include various incentives that directly support the security of these enterprises, and indirectly can be of other advantage as well (e.g., commercially).

1.4.2. The Five Mandates of National Cyber Security[122]

Within the general context of discussing national cyber security, it is important to keep in mind that this is not one single subject area. Rather, it is possible to split the issue of NCS into five distinct perspectives or 'mandates', each of which could be addressed by different government departments. This split is not an ideal state

[120] The 'Forum of Incident Response and Security Teams' (FIRST) is an international certification organisation for Computer Emergency Response Teams (CERTs, sometimes CSIRTs). CERTs are the principle organisation form for dealing with all manner of technical cyber security tasks and national CERTs that wish to belong to FIRST must be certified by the organisation.

[121] As an example, the US government interaction with part of worldwide technical CERT community is largely managed by the non-governmental Carnegie-Mellon University.

[122] See Section 4.3 for additional details. Based on Klimburg in Alexander Klimburg and Philipp Mirtl, Cyberspace and Governance – A Primer (Working Paper 65), (Vienna: Austrian Institute for International Affairs, 2012), http://www.oiip.ac.at/publikationen/arbeitspapiere/publikationen-detail/article/92/cyberspace-and-governance-a-primer.html.

but it is a reality due to the complexity and depth of cyber security as a whole. Each mandate has developed its own emphasis and even its own lexicon, despite the fact that they are all simply different facets of the same problem. Unfortunately, there is frequently a significant lack of coordination between these mandates, and this lack of coordination is perhaps one of the most serious organisational challenges within the domain of national cyber security.

Military Cyber: the internet security company McAfee has been warning since 2007 that, in its opinion, a 'virtual arms race' is occurring in cyberspace with a number of countries deploying cyber weapons.[123] Many governments are building capabilities to wage cyber war,[124] while some NATO reports have claimed that up to 120 countries are developing a military cyber capability.[125] These capabilities can be interpreted as simply one more tool of warfare, similar to airpower, which would be used only within a clearly defined tactical military mission (for instance, for shutting down an air-defence system). Military cyber activities, therefore, encompass four different tasks: enabling protection of their own defence networks, enabling Network Centric Warfare (NCW) capabilities, battlefield or tactical cyber warfare, and strategic cyber warfare.

Counter Cyber Crime: cyber crime activities can include a wide swathe of activities that impact both the individual citizen directly (e.g., identity theft) and corporations (e.g., theft of intellectual property). At least as significant for national security, however, is the logistical support capability cyber crime can offer to anyone interested in conducting cyber attacks. This is also where cyber crime interacts not only with military cyber activities, but also with cyber terrorism. As of 2012, there has not occurred any event that would be considered a 'cyber terrorist' attack despite, for instance, threats by the hacker group Anonymous to 'bring down the internet.'[126] This said, there have been a rising number of criminal acts, including attempts at mass disruption of communications, and this suggests cyber terrorism will be an issue for the future.

Intelligence and Counter-Intelligence: distinguishing cyber espionage from cyber crime and military cyber activities is controversial. In fact, both missions depend on similar vectors of attack and similar technology. In practice, however, serious espionage cases (regarding intellectual property as well as government secrets) are in a class of their own, while at the same time it can be very difficult to ascertain for sure if the perpetrator is a state or a criminal group operating on behalf of a

[123] See Zeenews, 'US, China, Russia have 'cyber weapons': McAfee,' *Zeenews.com*, 18 November 2009.

[124] See Michael W. Cheek, 'What is Cyber War Anyway? A Conversation with Jeff Carr, Author of 'Inside Cyber Warfare',' *The new new Internet*, 2 March 2010.

[125] See Julian Hale, 'NATO Official: Cyber Attack Systems Proliferating,' *DefenceNews*, 23 March 2010.

[126] Tyler Holman, 'Anonymous threatens to bring down the internet,' *Neowin.net*, 27 March 2012.

state, or indeed operating on its own. Whoever is actually behind the attack, cyber espionage probably represents the most damaging part of cyber crime (if included in the category). Cyber espionage, when directed toward states, also makes it necessary to develop specific foreign policy response mechanisms capable of dealing with the inherent ambiguity of actor-nature in cyberspace. At the same time, counter-intelligence activities (i.e., detecting and combating the most sophisticated cyber intrusions) very often will depend upon other types of intelligence activity, including human intelligence, signals intelligence, forensic analysis, etc., as well as extensive information sharing between international partners.

Critical Infrastructure Protection and National Crisis Management: critical infrastructure protection (CIP) has become the catch-all term that seeks to involve the providers of essential services of a country within a national security framework. As most of the service providers (such as public utilities, finance or telecommunications) are in the private sector, it is necessary to extend some sort of government support to help protect them and the essential services they provide from modern threats. While the original focus of these programmes post-September 11, 2001 was often on physical security, today the majority of all CIP activity is directly connected to cyber acts, usually cyber crime and cyber espionage. In this context, National Crisis Management must be extended by an additional cyber component. This includes institutional structures which enhance the cooperation between state and non-state actors both nationally and internationally, as well as a stable crisis communication network and an applicable legal framework to exchange relevant information.[127]

'Cyber Diplomacy' and Internet Governance: if diplomacy at its core is about how states exchange, deal with, gather, assess, present and represent information,[128] cyber diplomacy is about 'how diplomacy is adapting to the new global information order.'[129] Within this context, the promotion of aims such as 'norms and standards for cyber behaviour' (discussed primarily within the UN) and the aim for promoting 'confidence building measures between nations in cyberspace' needs to be understood as a mostly bilaterally-focused activity. Internet governance, in contrast, is largely a multilateral (or even multi-stakeholder) activity, and is probably the most international of all mandates. Internet governance is generally referred to as

[127] See, for instance, Austrian Federal Chancellery, *National ICT Security Strategy Austria* (Vienna: Digital Austria, 2012). 14-5.

[128] Adapted from Hedley Bull, *The Anarchical Society: A Study of Order in World Politics* (Basingstoke: Macmillan, 1977). 170-83.

[129] Evan H. Potter, ed. *Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century* (Quebec: McGill-Queen's University Press, 2002), 7. Potter originally is discussing 'e-diplomacy', which however in this Manual is defined as the ability to conduct diplomacy with cyber means.

the process by which a number of state and non-state actors interact to manage what, in effect, is the programming (or code, or 'logical') layer of the internet.

The above segmentation is an attempt to provide for a more structured discussion on the scope of national cyber security. The reality of these different mandates is that they are each dealt with by different organisational groups not only within government, but also within the non-state sector. Normatively speaking, all of these mandates should be holistically engaged if a comprehensive NCS perspective is to be developed.

1.5. THE FIVE DILEMMAS OF NATIONAL CYBER SECURITY

National cyber security is a tool to reach a desired state of affairs, not an end in itself. Most nations define a strategic goal of a safe and secure environment within which they can achieve full economic potential, and protect citizens from various cyber and non-cyber related risks, both domestic and foreign. To achieve this, NCS has to deal with its own, overarching set of 'national cyber security dilemmas'. In international relations theory, the traditional 'security dilemma' states that both a country's security strength and its weakness can create unfavourable reactions in their adversaries.[130] The NCS Dilemmas are, however, different: both a strong and a weak NCS posture can have economic and social costs.

1.5.1. Stimulate the Economy vs. Improve National Security

Nations are constantly facing the twin tensions of how to expedite the economic benefits of ICT and the internet economy while, at the same time, protecting intellectual property and privacy (data protection), securing critical infrastructure, and providing for defence of the homeland. The productivity promise that ICT brings for some nations will approach 10% of their GDP by 2015.[131] This growth is being documented in policies and funded through initiatives around the world. For example, the European Union is pursuing the Digital Agenda, the United States is pursuing the Innovation Agenda, and China is pursuing a policy of

[130] See, for instance, Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976). 66-72.

[131] Soumitra Dutta and Irene Mia, The Global Information Technology Report 2009-2010. ICT for Sustainability, (Geneva: World Economic Forum, 2010), http://www3.weforum.org/docs/WEF_GITR_Report_2010.pdf. 12 and 61. See also Scott C. Beardsley et al., 'Fostering the Economic and Social Benefits of ICT,' *The Global Information Technology Report 2009-2010* (Geneva: World Economic Forum, 2010), http://www3.weforum.org/docs/WEF_GITR_Report_2010.pdf; Dean et al., 'The Connected World: The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy.'

'Informationisation'. The agendas have common components: provision of high-speed internet to citizens and businesses modernisation of critical infrastructures with new ICT components that can communicate with the internet and promotion of research and innovation to ensure that innovative ideas can be turned into products and services that create growth and jobs and, ultimately, drive competitiveness. Businesses and governments embrace the efficiency savings that ICT presents and are accelerating the pace and mechanisms by which transactions and services are conducted over the internet. Businesses are using just-in-time manufacturing and retail distribution, and essential services like electricity, water, and fuel supply are increasingly being managed over the internet. ICT is the platform for innovation, prosperity and advancing a nation's economic and national security interests.

The success of a nation's ability to leverage ICT to achieve the desired economic stimulus and social benefits should depend on its use of the different market levers to assure the confidentiality, integrity and availability, and the security of networks and information systems that are central to the economy and society. The most important issue, however, remains, simply put, cost – it supersedes all other concerns, including those of security. This is certainly short-sighted: the advances of ICT can be more than off-set through ICT-amplified disasters. The security of the ICT hardware supply chain, for example, is a well-known issue but an issue where there are seemingly no simple and, most importantly, no cheap solutions.[132]

Despite increasing awareness of the associated risks, consumers and large businesses do not take advantage of available technology and processes to secure their systems, nor do they take protective measures to blunt the evolving threat. This general lack of investment puts firms and consumers at greater risk, leading to economic loss at the individual and aggregate level and thus poses direct a threat to national security.[133] Three issues are central to the national security debate: how does the government assure the availability of essential services; provide for the protection of intellectual property; and maintain citizen confidence (and safety) when participating in the internet economy? Nations are struggling with finding the appropriate mix of policy interventions and market levers to boost the impacts of ICT. Connectivity among individuals, businesses and markets demand more robust security to reduce consumer risk and enable organisations to offer better service and increased capabilities online. Policy intervention (both regulatory and

[132] One programme intended to provide 'trusted' microchips for sensitive US ICT systems is the 'Trusted Foundry Program' (Catherine Ortiz, 'DOD Trusted Foundry Program: Ensuring 'Trust' for National Security & Defense Systems,' in *NDIA Systems Engineering Division Meeting* (Arlington, VA: Trusted Foundry Program, 2012).).

[133] US Department of Commerce, Cybersecurity, Innovation, and the Internet Economy (Green Paper), (Gaithersburg, MD: NIST, 2011), http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf.

incentives based) must harness the capabilities and responsibilities of the private sector to achieve a prudent level of security without hindering productivity, trade or economic growth.

1.5.2. Infrastructure Modernisation vs. Critical Infrastructure Protection

A key tension that stems from the economic vs. national security debate is the tension between the forces that are driving infrastructure modernisation (economic stimulus) *vis-à-vis* the forces that are demanding critical infrastructure protection.[134] These infrastructures are being modernised, harnessing affordable access to broadband applications and services, and inexpensive ICT devices. As such, they increasingly comprise a heterogeneous composite of hardware and software products that, for the most part, combine unverified hardware and software that is manufactured by a heterogeneous global industry using global distribution channels.

Businesses are capturing the ICT dividend; gaining efficiency and productivity but perhaps at the expense of basic security. Owners and operators of these infrastructures (e.g., water, finance, communications, transportation and energy installations and networks) are first and foremost worried about providing returns for shareholders, whereas a government's concern is with overall public security and safety.[135] Governments recognise that a disruption in one infrastructure can easily propagate into other infrastructures and that they are responsible for protecting the nation from catastrophic damage. Perhaps this is why, 'critical infrastructure services are regarded by some governments as national security related services.'[136]

The short-term economic gains of adopting new technologies and transforming the cyber infrastructure must be balanced against the medium and longer-term losses stemming from failing to adequately secure these systems and infrastructures.[137] While there a number of examples of this, the current discussions around modernising the electric power sector to internet-facing 'smart grids' is emblematic:

[134] 'Critical infrastructures are those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments' (See European Union, 'Critical infrastructure protection,' http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm.).

[135] Peter Sommer and Ian Brown, Reducing Systemic Cybersecurity Risk, (Paris: OECD, 2011), http://www.oecd.org/sti/futures/globalprospects/46889922.pdf.

[136] ISO/IEC 27032:2012, 'Information technology – Security techniques – Guidelines for cybersecurity,' 11.

[137] Jack Goldsmith and Melissa Hathaway, 'The cybersecurity changes we need,' *The Washington Post*, 29 May 2010.

while the industry would reap great productivity gains, there are a number of serious unsolved security concerns. For example, 'smart meters with designated public IP addresses may be susceptible to denial of service attacks which could result in loss of communication between the utility and the meters and therefore deny power to homes and businesses.'[138] Thus, a potential 'modernisation' agenda is brought into direct conflict with a security agenda.

Deploying appropriate security measures to manage risk to critical systems and assets is costly. The question is: what are the most appropriate and effective security measures to manage risk to critical systems and assets and who pays for it? Owners and operators of these infrastructures have to play an active role in defining the standards that must be implemented to meet the government's mandate in assuring essential services. Industry also may be asked to make security investments that go beyond what is required to meet compliance and regulatory regimes. The policy intervention that a government uses to meet the needs of the nation must be carefully balanced to heighten cyber security without creating barriers to innovation, economic growth, and the free flow of information.

1.5.3. Private Sector vs. Public Sector

A critical feature of modern NCS is the role of the private sector. It is responsible for the research, design, development and manufacturing of the vast majority of software and hardware used in ICT. It has, in effect, become 'the' service provider; the steward of the internet that plans and manages resources, provides reliable connectivity, and ensures delivery for traffic and services.

Critical infrastructures and industries are increasingly the primary target of cyber crime, cyber espionage, and, most recently, serious cyber attack. Their electronic defences have been punctured and the potential costs of these activities are considerable. For example, the theft of intellectual property (which includes cyber espionage activity) is said to have cost the UK economy up to £9.2 billion in 2010.[139] Some adversaries have ambition to destroy or, perhaps worse, deliberately insert erroneous data to render systems inoperable and information unusable. The costs of these activities against the critical infrastructure are difficult to estimate, however, one industry report claimed that in the US 'the reported costs of downtime due

[138] Melissa Hathaway, 'Power Hackers: The U.S. Smart Grid Is Shaping Up to Be Dangerously Insecure,' *Scientific American*, 5 October 2010, 16.

[139] Detica, The Cost of Cyber Crime. A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office, (London: UK Cabinet Office, 2011), http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf.

to cyber attacks exceed $6 million a day'.[140] In April 2009, the North American Electric Reliability Corporation (NERC) issued a public notice that warned that the electrical grid is not adequately protected from cyber attack: 'facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.'[141] Some observers have warned that a serious cyber attack on the US electrical grid could cause 'over $6 billion in damages,'[142] and the Commander of US Cyber Command said that, between 2009 and 2011, attacks on US critical infrastructures had 'risen 20-fold.'[143]

Governments have a clear interest in assisting the private sector in protecting the nation's essential services, wealth and growth potential (e.g., intellectual property protection) from these activities, but the ways and means of this assistance is fiercely debated. For example, some governments are choosing to regulate critical infrastructure providers by imposing minimum standards for technology deployment, internal security controls, and disaster recovery and business continuity plans. Whereas other government intervention options may include the provision of tax incentives, stimulus grants, low-cost or no-cost loans, government subsidies, insurance, and even liability protection. These incentives are meant to encourage industry participation in meeting the desired infrastructure objectives – to be both secure and resilient.

Either one of these options usually is supported by information exchanges, sometimes also referred to as the private-public partnership, that draw on combining the best of both party's understanding of the environment to support operational cyber security. For example, in some cases this includes pooling knowledge of tactics, techniques and procedures used to probe and successfully breach corporate and government networks.[144] Other information exchanges share counter-measure technologies and solutions to deny or investigate the cyber perpetrator.[145] Some governments even offer to help protect their critical infrastructure directly, by deploying sensors in the networks to (supposedly) detect the most advanced

[140] Stewart Baker, Shaun Waterman, and George Ivanov, In the Crossfire. Critical Infrastructure in the Age of Cyber War, (Santa Clara, CA: McAfee, 2010), http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf.

[141] Michael Assante, Critical Cyber Asset Identification [Letter to Industry Stakeholders], (Princeton, NJ: NERC, 2009), http://www.nerc.com/fileUploads/File/News/CIP-002-Identification-Letter-040709.pdf.

[142] John O. Brennan, 'Time to protect against dangers of cyberattack,' *The Washington Post*, 16 April 2012.

[143] Jasmin Melvin, 'White House lobbies for cybersecurity bill amid worries it may stall,' *Reuters*, 1 August 2012.

[144] See Critical Infrastructure Protection Initiative (CPNI): http://www.cpni.gov.uk/about.

[145] INTERPOL, 'INTERPOL and ICANN advance cooperation on Internet security after historic first meeting,' *Media Release*, 23 May 2011.

threats.[146] These can be accompanied by encouraging the developments of voluntary codes of conduct, creating repositories of best practices, and encouraging private-sector initiatives to regularly test their systems' security posture and practice their recovery processes and procedures. Each of these initiatives helps build trust and understanding among and within the partnership and, perhaps more importantly, begins to promote education and awareness-raising across the nation.

While it remains unclear to what extent these measures actually help protect private business and the nation's networks, an equally contentious debate is being waged around the governmental approach to intervention in the private sector: either seeking voluntary cooperation or 'mandated' (i.e., prescribed by law or regulation). Understandably this involvement of the state in private affairs is a deeply ideological question in many nations. According to one 2009 study on European CIIP programmes,[147] of 16 EU Member States examined, around half favoured more voluntary than mandatory principles in their programmes, approximately six balanced voluntary and legal measures, and only two Member States seemed to largely or completely dependent on regulation. It is however very likely that this number has changed, given the recent European trend for applying legislation to the issue.

Most nations, however, agree that cyber security is a shared responsibility. The Director of the UK Government Communications Headquarters (GCHQ) recently argued that it is this 'holistic approach to cyber security that makes UK networks intrinsically resilient in the face of cyber threats.'[148] He went on to explain that this enhanced security posture would lead to a more competitive, economic posture for the nation.

1.5.4. Data Protection vs. Information Sharing

Another barrier to realising the full economic benefits of the internet economy involves the natural conflict between citizens' expectations and government policy for data protection and preserving privacy *vis-à-vis* the need to share information across boundaries and borders (e.g., government to industry, government to government, industry to industry) with the intent to enhance security. Enterprises of all kinds rely on the willingness of consumers and business partners to entrust them with private information. These constituents, in turn, expect that this information will stay both private and secure. Citizens expect protection from

[146] Warwick Ashford, 'BT extends cyber security agreement with MoD,' *ComputerWeekly.com*, 4 July 2012.

[147] Booz & Company, *Comparison and Aggregation of National Approaches (JLS/2008/D1/019 – WP 4)* (2009). 28.

[148] BBC, 'UK infrastructure faces cyber threat, says GCHQ chief,' *BBC News*, 12 October 2010.

intrusions by both private and governmental actors. In 1980, the OECD issued a 'Recommendation Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.'[149] The OECD guidelines influenced international agreements, national laws and self-regulatory policies.

This document sparked discussion around the world and, over the next three decades, different approaches to privacy policy and regulation emerged for reasons ranging from enhancing national security to negatively impacting economic growth. As one industry expert noted, 'providing seamless privacy protection for data as it flows through the global internet requires a careful reconsideration of the business community's interest in promoting commerce, the government's interests in fostering economic growth and protecting its citizens, and the interest of individuals in protecting themselves from intrusive overreach by government and the private sector.'[150] Today, many governments have established privacy rights for individuals, developed data protection frameworks and mandated privacy policies to preserve this notion of confidentiality.

Yet, countering crime, espionage, and other illicit activities in cyberspace demands timely exchange of warnings and follow up information among and between private and public entities, often exchanging sensitive data that may fall within the remit of these privacy and data protection laws. A major example of this dichotomy could be seen in Europe, where the 'European Data Retention Directive' (EDRD)[151] was in some ways the one of the most controversial pieces of EU legislation ever passed, and indeed is still being resisted by some EU Member States. Computer incident response centres and industry information security specialists argue that they need an information sharing mechanism that swiftly delivers alerts regarding tactics, techniques, and procedures used to probe and successfully breach victim networks. For some countries, this falls within the private-public partnership cooperation models where industry and government share the responsibility for security and resilience objectives. For example, the United States, the United Kingdom and other governments are providing actionable information and analysis regarding current threats to their industry. While not robust, these initiatives are trying to establish bi-directional information sharing architectures to accelerate better understanding or situation awareness about how industry or the nation overall is being targeted, what information is being lost, and the methods they

[149] OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD, 1980).

[150] CDT, 'Chapter Three: Existing Privacy Protections,' ed. CDT, *CDT's Guide to Online Privacy* (Washington, DC: CDT, 2009), https://www.cdt.org/privacy/guide.

[151] The EDRD was adopted in 2006 and requires, among other things, that all ISPs keep their customer logs six months to two years to support criminal prosecution.

(industry and government) can use to defend their information assets, and respond to, and recover from significant incidents.

National laws may be insufficient, on their own, to provide citizens with privacy protections across borders while at the same time allowing for the timely exchange of threat information. This inherent tension lies at the heart of the cyber security debate.

1.5.5. Freedom of Expression vs. Political Stability

Recent news reports have illustrated how ICT and innovative use thereof can enhance or constrain the power of politicians and the general public. For some, ICT allows for widespread participation by citizens in day-to-day policy decisions. For example, in January 2012, US politicians faced widespread outrage regarding the Stop Online Piracy Act (SOPA), a bill that was introduced and debated before Congress.[152] Opponents to the bill stated that the proposed legislation threatened free speech and enabled law enforcement to block access to the internet due to copyright infringing (anti-piracy) content posted on web pages or blogs. On January 18, 2012, Wikipedia, Reddit, TwitPic and an estimated 7,000 other smaller websites coordinated a service blackout to raise awareness. The bill was quickly postponed for consideration due to this public pressure. In August 2011, during the England riots, some rioters used Blackberry Messenger to organise their activities and others utilised Twitter and Facebook to coordinate clean-up operations.[153] British officials used facial recognition software with social networks like Facebook to allow citizens to report rioters to authorities. In addition, social networking helped identify suspects and apprehend them for criminal damage, burglary, and violent disorder. A wider 'crackdown' on social media was narrowly avoided.[154]

ICT innovations also raise privacy concerns because governments and corporations can use 'digital surveillance technologies, such as networked webcams, location tracking, digital identification (ID) devices, data mining and analyses of communication traffic and search engine queries' to create digital dossiers of our citizens.[155] Activist groups such as Anonymous, LulzSec and WikiLeaks, expose victim's data to embarrass or achieve other objectives. However, the United States continues to push for equal access to knowledge and ideas across the digital

[152] Ned Potter, 'Wikipedia Blackout,' SOPA and PIPA Explained,' *ABC News*, 17 January 2012.

[153] BBC, 'England riots: Twitter and Facebook users plan clean-up,' *BBC News*, 9 August 2011.

[154] See, for instance, Peter Apps, 'Analysis: UK social media controls point to wider 'info war',' *Reuters*, 18 August 2011.

[155] Walter S. Baer et al., Machiavelli Confronts 21st Century Digital Technology: Democracy in a Network Society (Working Paper), (Oxford: Oxford Internet Institute, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1521222. 5.

frontiers of the 21st century: 'This freedom is no longer defined solely by whether citizens can go into the town square and criticise their government without fear of retribution. Blogs, e-mail, social networks and text messages have opened up new forums for exchanging ideas – and created new targets for censorship.'[156]

New technologies are being used to change the outcomes in the struggle for freedom and progress. The internet can be co-opted as a tool to target and silence citizens and it can be used to deny access to and use of key applications. For example, in early April 2012, the Iranian minister for Information and Communications Technology announced that Iran will field a national Intranet and begin blocking services like Google, Gmail, Google Plus, Yahoo and Hotmail, in line with Iran's plan for a 'clean internet.' These 'Western' services will be replaced with government internet services like Iran Mail and Iran Search Engine.[157]

In addition, during the early days of the social uprising that ultimately lead to the ousting of President Hosni Mubarak, the Egyptian telecommunications authority received an order from the security services to shutdown internet access. 88% of Egyptians lost access to the internet during this episode.[158] Other states in the region (e.g., Libya and Syria) implemented similar measures to try to maintain social stability as the 'Arab Spring' continued. While the acts of authoritarian regimes fighting for their political lives may seem extreme to many in the Western world, what these episodes demonstrate is that the very interconnectedness that people around the globe enjoy because of improvements in ICT can be swiftly denied, and that freedom of communication and political freedom are clearly linked.

1.6. CONCLUSION

Addressing a nation's cyber security needs is no easy task. Indeed, it is not even always apparent what those needs exactly are, or what protecting (or not protecting) a nation's cyber environment actually entails. Quite often there are different and competing considerations within each nation's approach. Yet each nation is faced with a steadily increasing level of cyber threat, and thus requires the nation's leadership to recognise the strategic problem and set forth goals and strategies to address it. In this section we have defined NCS as 'the focused application of specific governmental levers (which includes both incentives and regulation) and information assurance principles to public, private, and relevant international

[156] Hillary R. Clinton, 'Internet Freedom [Speech at Newseum in Washington, DC],' *Foreign Policy*, 21 January 2010.

[157] Amrutha Gayathri, 'Iran To Shut Down Internet Permanently; 'Clean' National Intranet In Pipeline,' *International Business Times*, 9 April 2012.

[158] Christopher Williams, 'How Egypt shut down the internet,' *The Telegraph*, 28 January 2011.

ICT systems, and their associated content, where these systems directly pertain to national security.' As nations and intergovernmental organisations set about developing and implementing measures to establish NCS strategies, they must balance the economic and social importance of free flow of information to the security needs of government, industry, and citizens. The conceptual prism set forth in this section is designed to assist in this development and debate.