UNIDIR

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

INSTITUTE FOR PEACE RESEARCH AND SECURITY POLICY

UNITED NATIONS

UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

The Cyber Index

International Security Trends and Realities

UNIDIR/2013/3

The Cyber Index

International Security Trends and Realities

UNIDIR
United Nations Institute for Disarmament Research
Geneva, Switzerland

New York and Geneva, 2013

NOTE

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

*
* *

The views expressed in this publication are the sole responsibility of the individual authors. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

UNIDIR/2013/3

UNITED NATIONS PUBLICATIONS

The United Nations Institute for Disarmament Research (UNIDIR)—an autonomous institute within the United Nations—conducts research on disarmament and security. UNIDIR is based in Geneva, Switzerland, the centre for bilateral and multilateral disarmament and non-proliferation negotiations, and home of the Conference on Disarmament. The Institute explores current issues pertaining to the variety of existing and future armaments, as well as global diplomacy and local tensions and conflicts. Working with researchers, diplomats, government officials, NGOs and other institutions since 1980, UNIDIR acts as a bridge between the research community and governments. UNIDIR's activities are funded by contributions from governments and donor foundations.

www.unidir.org

CONTENTS

ACKNOWLEDGMENTS

Thanks to Kerstin Pertermann who helped to collect, structure, and prepare the text on international organizatons and confidence-building.

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities.

In addition, dedicated project funding was received from the Government of Germany.

ABOUT THE AUTHORS

James Andrew Lewis is a senior fellow and Program Director at the Center for Strategic and International Studies. Before joining the Center, he worked at the US Departments of State and Commerce as a Foreign Service Officer and as a member of the Senior Executive Service. He was the Rapporteur for the 2010 United Nations Group of Governmental Experts on Information Security. Lewis's recent work has focused on cybersecurity, including the ground breaking "Cybersecurity for the 44th presidency". Recent reports include "Thresholds for cyber warfare", "Deterrence and credible threats", "Internet governance and cybersecurity", "Multilateral agreement to constrain cyber conflict", and "Privacy and cybersecurity". His current research examines strategic competition and technological innovation. Lewis received his PhD from the University of Chicago.

Götz Neuneck is Deputy Director of the Institute for Peace Research and Security Policy at the University of Hamburg. Trained as a physicists at the University of Düsseldorf, he received his PhD in mathematics at the University of Hamburg, and since 2007 is a professor at the Faculty of Mathematics, Informatics, and Natural Sciences at the University of Hamburg. Since 2001 Neuneck is speaker of the Physics and Disarmament Working Group of the German Physical Society and a member of the Council of the Pugwash Conferences on Science and World Affairs. His current areas of work are nuclear arms control and disarmament, ballistic missile defence, space/cybersecurity, and non-proliferation of military technology.

FOREWORD

Today, cyberspace is part of the daily life of many citizens, communities, industry, academia, and governments around the world. Moreover, the global expansion of digital media, networks, and information and communications technologies (ICTs) might well become the most powerful technological revolution in the history of humankind. Social media, internet shopping, and online banking are becoming ever more popular, creating a powerful economy while enabling borderless exchange of information and media. In 1993, only 50 Internet websites existed; this number increased to 555 million in 2011 and will continue to grow. The Internet facilitates free speech and the exchange of information, the propagation of the use of modern technologies, and free trade.

The early development of the Internet was very much determined by insider communities of technologists and private sector actors. Due to the rapid pace of technological development, the increase in use of ICTs, and the rapid expansion of internet access, many political, legal, and societal aspects of the cybersphere are not yet fully understood. But it is clear that multilateral debate must focus not only on future cyber threats and acceptable responses, but also on individual and state rights in the cyber domain, the question of future internet governance, and the role of civil society, governments, and the military in securing the cybersphere.

The benefits to states, communities, and individuals of the cybersphere are clear. The "Information Revolution" has given the global community the capability to rapidly and easily connect individuals, companies, governments, international institutions, and other entities. Interconnectivity via digital networks is the key characteristic of today's global economy, and is increasingly required for global economic stability and development.

However, these benefits come with risks and costs. Civil society, the private sector, governments, and militaries are increasingly dependent on networked ICTs, which creates new vulnerabilities to national and global security. Indeed, we have seen steady annual growth in cybercrime and other types of malfeasance in the cybersphere in tandem with the expansion of use. According to internet security firm Symantec, web-based attacks increased in 2011 by 36 per cent over 2010, with more than 4,500

new attacks each day. Some 403 million new variants of malware were created in 2011, a 41 per cent increase over 2010.[1]

Cyberattacks are often defined broadly as the unauthorized penetration of computers or digital networks. Cyberattacks are occurring every day, ranging from website defacement, to denial-of-service attacks, to the theft of data and infiltration of computers and servers. Based on malware or corrupted programs, these activities range from manipulating passwords, to stealing data, to hijacking computers for a variety of illegal purposes (through tools such as botnets), to disrupting services. Cyberattacks are intended to prevent users from access to services or to disrupt computer-controlled machines, while cyber exploitation is conducted to penetrate computers to obtain information.[2] Most of these attacks do not cause physical damage, but instead often result in economic loss—and sometimes to increasing tensions among states. Cyberattacks worldwide are becoming more complex and frequent, and the economic damage caused is increasing.

Government efforts to protect infrastructure and undertake law enforcement in the cybersphere are complicated by the fact that most infrastructure and assets involved are owned and operated by private sector actors, who have widely diverse motivations and sometimes competing equities to protect. For example, efforts by the Obama administration to pass cybersecurity legislation have been battered by corporate interests seeking to avoid new regulatory burdens on one hand and, on the other hand, the concerns of many civil liberties organizations about protecting the privacy of citizens online.

The ubiquity and diversity of non-state actors in cyberspace—ranging from individuals concerned about internet freedom to politically motivated groups such as Anonymous to organized cybercriminals—further complicate efforts at governance. Attacks by non-state actors have not been limited to state-owned websites and governmental organizations. For example, in the aftermath of the 2010 WikiLeaks affair, and the refusal by many financial institutions to allow contributions to the site, "hacktivists" carried out a concerted campaign against those banks and corporations involved.

The highly sophisticated Stuxnet worm—discovered in 2010, and engineered primarily to attack Iranian uranium enrichment facilities—

1 Symantec, *Internet Security Threat Report*, 2012, pp. 11–12.

2 H. Lin, "Some modest steps toward greater cybersecurity", *Bulletin of the Atomic Scientists*, vol. 68, no. 5, 2012.

demonstrated for the first time that states can manipulate the industrial infrastructure of other states via malicious cyber tools. Stuxnet, uniquely, is viewed by many legal scholars as the equivalent of an "armed attack" under international law because it did actual physical damage, rather than simply manipulating data. Variants of Stuxnet such as Flame (discovered in 2012), or malware such as that used by the China-based GhostNet network to spy on a more than 100 countries, represent some of the new surveillance tools available to states or criminal enterprises. Countless espionage attacks are aimed at governments and industry to gain sensitive information in the defence and business sectors. Indeed, targeted attacks aimed at businesses and governments increased from 77 per day in 2010 to 82 per day in 2012, according to Symantec.[3] Allegations about cyberespionage also are increasingly bedevilling political and economic relations among states.

The cyberattacks against Estonia 2007 and during the Russian–Georgian conflict in 2008 served to raise international concern regarding the use of cyberattacks as disruptive tools in future warfare. Undoubtedly, the Internet already is becoming a zone of potential conflict as states step up military capabilities. While the use of cyberattacks in conjunction with armed conflict now seems likely, there remains disagreement among states as to the extent to which international law can or should be applied to the cyber domain.

In a number of states, serious policy debates are underway regarding potential military responses to threats in the cyber domain, such as preventive strikes with conventional weapons or cyber counterattacks that could destroy, deny, disrupt, or corrupt an adversary's attempt to use cyberspace for a military attack. According to the *New York Times*, the militaries of some states consider "disruptive software" as an "essential new tool of war", noting that the 15 states with the largest military budgets are all investing in offensive cybercapabilities.[4]

At the same time, national, regional, and international efforts are underway to assess the risks associated with military use of cyber offence, as well as issues of how international law would apply to such use. The NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, has for example recently issued a manual interpreting principles of jus ad bellum, which regulates the use of force, and jus in bello, which governs

3 Symantec, *Internet Security Threat Report*, 2012, p. 14.

4 "A new kind of warfare", *New York Times*, 9 September 2012.

the conduct of armed conflict.[5] The concept of confidence-building and security measures is also being discussed in a number of multinational forums.

The United Nations and several regional organizations—including the Association of Southeast Asian Nations Regional Forum, the Organization for Security and Cooperation in Europe, the European Union, and the North Atlantic Treaty Organization—have launched formal processes designed to find multilateral approaches to securing the cyber domain and avoiding threats to international security that may emanate from its use.

It is our intention that this study serve as a "snapshot" of current cybersecurity activities at the national, regional, and international levels, to help policymakers and diplomats understand the complexity of the arena. In addition, the study seeks to elucidate some approaches towards mitigating the risks of misperceptions in the cyber domain that threaten to elevate international tensions or perhaps even lead to conflict. The subject matter, of course, is multifaceted, highly complicated, and controversial—thus no one study could adequately cover all aspects in depth. Nonetheless, we hope that this study will at a minimum help underpin ongoing discussions and debates by providing facts and fact-based analysis of today's challenges and opportunities regarding international stability and security in the cyber domain.

Theresa Hitchens, Director
United Nations Institute for Disarmament Research

James Andrew Lewis
Center for Strategic and International Studies

Götz Neuneck
Institute for Peace Research and Security Policy at the University of Hamburg

5 "The Tallinn Manual", NATO Cooperative Cyber Defence Centre of Excellence, www.ccdcoe.org/249.html.

INTRODUCTION

Cybersecurity is a global concern, reflecting the central importance of cyberspace for business, politics, and security. It has been an issue of concern for international security at least since 1998, when the Russian Federation first proposed a treaty in the United Nations General Assembly to reduce the risk of cyberconflict. At that time, only a few states had national programmes for cybersecurity or cyberwarfare in place. Now, more than half of all United Nations Member States have some kind of national effort to secure critical networks and to respond to cyber threats.

In the first chapter of part I, national cybersecurity efforts are divided into two general categories: those involving only domestic agencies (usually communications ministries or law enforcement agencies) and those where the national military has a cybersecurity role. The first section lists those states for which there is public information on a military role in cybersecurity including, in some instances, the development of offensive capabilities. The second section lists those states for which there is public information on cybersecurity as a civilian task.

The initial assessment undertaken in 2011 found that 68 of the 193 United Nations Member States had cybersecurity programmes.[6] Of those, 32 states included cyberwarfare in their military planning and organizations, while 36 states had civilian agencies charged with a domestic cybersecurity mission. This August 2012 assessment again surveyed publicly available information for the 193 states and found that the number of national cybersecurity programmes had grown to 114. Forty-seven states have cybersecurity programmes that give some role to the armed forces and 67 states have solely civilian programmes.

This assessment is based in publicly available sources from the states in question, from national media, published government sources, or, in some cases, government reports to multilateral organizations.[7] It is important to note that transparency in cybersecurity efforts is limited, particularly

6 Center for Strategic and International Studies, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*, UNIDIR, 2011.

7 The three exceptions to this are Cuba, the Democratic People's Republic of Korea, and Myanmar.

when it comes to the military use of cyber techniques, and much of the publicly available information is incomplete and uneven, reflecting the limited information that governments make available. Only six states have published military cyber strategies (with varying degrees of detail and specificity). Two other states plan to issue military cyber strategies. A further 30 identify cybersecurity as a military concern or priority in policy documents (usually as part of national military strategies or national defence white papers). These documents identify areas of military responsibility and missions, but other information—on doctrine for use, command and control, budget, or cybercapabilities—is sparse or non-existent. A decision by governments to increased transparency in these areas could have a stabilizing effect in the international community, or at least help to identify issues that require greater attention.

States in all regions of the world now have cybersecurity initiatives, reflecting regional mandates (particularly in Europe), multilateral and bilateral discussions, or efforts at assistance in developing national programmes. Published information shows that 18 states in Africa have cybersecurity programmes,[8] 16 states in the Americas,[9] 39 states in Asia,[10] 38 states in Europe,[11] and 3 states in Oceania.[12] Unsurprisingly, it is among

8 Burundi, Cameroon, Egypt, Ethiopia, Ghana, Kenya, Madagascar, Mauritius, Morocco, Nigeria, Rwanda, South Africa, Sudan, Swaziland, Tunisia, Uganda, United Republic of Tanzania, and Zimbabwe.

9 Antigua and Barbuda, Argentina, Brazil, Canada, Colombia, Cuba, Dominican Republic, Grenada, Jamaica, Mexico, Panama, Peru, Saint Vincent and the Grenadines, Trinidad and Tobago, United States, and Uruguay.

10 Afghanistan, Armenia, Azerbaijan, Bangladesh, Bhutan, Brunei Darussalam, Cambodia, China, Cyprus, Democratic People's Republic of Korea, Georgia, Indian, Indonesia, Iran (Islamic Republic of), Israel, Japan, Jordan, Kazakhstan, Kuwait, Lebanon, Malaysia, Maldives, Mongolia, Myanmar, Nepal, Oman, Pakistan, Philippines, Qatar, Republic of Korea, Saudi Arabia, Singapore, Sri Lanka, Syrian Arab Republic, Thailand, Turkey, United Arab Emirates, Viet Nam, and Yemen.

11 Albania, Austria, Belarus, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Montenegro, Netherlands, Norway, Poland, Portugal, Republic of Moldova, Romania, Russian Federation, Serbia, Slovakia, Slovenia, Spain, Switzerland, Sweden, Ukraine, and United Kingdom.

12 Australia, Fiji, and New Zealand.

the smaller and less-developed countries where no reference to national cybersecurity efforts could found.

The most dramatic increase since 2011 is in the number of states for which information was found showing the development of domestic cybersecurity programmes to protect networks and critical national infrastructures, with the number increasing from 36 to 67. Many of these national programmes involved the most basic steps, such as passing cybercrime legislation, improving law enforcement capabilities, or creating a computer emergency response team (CERT). States with more advanced cybersecurity programmes have developed strategies to protect critical infrastructure and have established dedicated organizations to carry out this responsibility.

In contrast to the growth in civilian programmes, only nine states have added military cyber programmes—41 states now have publicly acknowledged some military planning or specific military organizations for cyber activities. It appears that states are in a period of experimentation as they assess the risks and benefits of these new military capabilities, and as they develop strategies, doctrine, and organizations to best use them. The most advanced militaries are creating specific and dedicated military organizations for cyberwarfare. The 2011 assessment identified 12 states that had established or planned to establish specific military cyberwarfare entities. By 2012, that number had grown to 27, and of these, media reports indicate that 17 are developing offensive cybercapabilities. It is likely that other states are pursuing similar organizational experiments on a covert basis.

The assessment indicates, unsurprisingly, that states with large defence budgets are most likely to invest in developing cyberwarfare capabilities. The publicly available information suggests that 12 of the 15 largest military spenders have or are developing dedicated cyberwarfare units. Open-source information suggests that of these 12 states, 10 appear to possess or be developing offensive cybercapabilities. This growing military dimension makes cybersecurity an essential subject for discussion and negotiation on international security at both the regional and global level.

Cooperation on cybercrime, including cooperative efforts to develop effective national legislation, is also a major focus for national efforts, given cybercrime's transnational nature and the close relationship between crime and national security in cyberspace—the same tools used for crime can be used for espionage or attack, and often cybercriminals can be recruited

to serve national purposes. The international community has recognized the importance of controlling cybercrime and has developed a number of multilateral instruments (sometimes cooperative, sometimes competing) to address it. Among the international agreements that could provide a foundation for cooperation on cybercrime, the Convention on Cybercrime has the greatest degree of support. Thirty-three states have ratified it, 11 are signatories, and another 10 have expressed their intention to sign, making the convention the de facto standard for cybercrime.

The elements of international cybersecurity—cooperation in building domestic security, the expansion of military capabilities, and law enforcement—present a robust agenda for multilateral work. Progress in building cooperation will take time and effort at many different levels of engagement. One encouraging development in recent years is the rapid growth of multilateral efforts, on the part of, among others, the Shanghai Cooperation Organization, the Organization of American States, the Asia–Pacific Economic Cooperation Forum, the Association of Southeast Asian Nations Regional Forum, the Economic Community of West African States, the African Union, the European Union, the Organization for Security and Co-operation in Europe, the Group of 20, the North Atlantic Treaty Organization, and the Council of Europe. Capping these efforts, the work of the United Nations in the General Assembly, the committees and the Secretary General's Group of Governmental Experts provides a global underpinning to regional work. Chapter 2 of part I provides an overview of international and regional organizations and their activities.

The information found on cybersecurity programmes points to key issues at both the national and international level. These include a growing need for coordination, regionally and globally, among the many national programmes. Given the degree and speed of interconnectivity among states in cyberspace, a purely national approach to cybersecurity could never be adequate for national defence or to meet existing obligations under international law. Creating a CERT or a cybercrime unit, while a useful first step, is inadequate to protect infrastructure and information since CERTs and cyber police are often reactive rather than preventive. States cannot behave as if cybersecurity does not have a military dimension or that somehow it will be possible to eliminate or ban military and espionage cybercapabilities— recognition of this imposes new responsibilities upon individual states and the international community. As with others areas of cybersecurity, an immediate goal is to raise the level of discussion and decision-making from the technical to the political level.

Even with the limitations of publicly available data, this assessment confirms that cybersecurity and the military use of cyber techniques has become a central element for any discussion of national and international security. Stronger national policies and a cooperative framework of rules and understandings are needed to guide use and to reduce concern over cybersecurity. Current international understandings, structures, and institutions for cybersecurity are undeveloped and inadequate. As part II, chapter 2, of this study details, there are precedents from arms control negotiations and non-proliferation that may help to accelerate progress in making cyberspace more secure, but there are serious differences among states regarding political relations, human rights, trade, and warfare, and we are far from consensus. Part II, chapter 3, looks at some first steps towards international cooperation to secure cyberspace, specifically at embryonic efforts to create confidence- and security-building measures among states as a foundation for improved cooperation. As national programmes for both domestic security and military action continue to grow in number, resolving these issues will be a task that all states will share.

PART I

CHAPTER 1

CYBERSECURITY AND CYBERWARFARE: ASSESSMENT OF NATIONAL DOCTRINE AND ORGANIZATION

James Andrew Lewis

STATES WITH MILITARY DOCTRINE, POLICIES, OR ORGANIZATIONS

Albania

Albania views cyberattack as an emerging threat and is drafting a national cyber strategy. A Cyber Coordinator will be located in the prime minister's office. In 2010, the Albanian Ministry of Defence created the Inter-Institutional Maritime Operational Center, with responsibility for civil emergencies, airspace control, and developing a cyberdefence capability.[13] In 2011, the United States and Albania launched a joint initiative under United States Agency for International Development to improve Albania's ability to prevent and respond to cybersecurity incidents.[14] As part of the programme, Albanian officials attended workshops held by the Carnegie Mellon Software Engineering Institute to assist the Albanian government in creating a national computer emergency response team (CERT).[15]

Argentina

Argentina has both civilian and military agencies with a cybersecurity mission. Argentine military officials have stated that information warfare capabilities should include both defensive measures to protect domestic

13 See Albanian Ministry of Defence, "Interinstitutional Maritime Operational Centre", www.mod.gov.al/eng/index.php?option=com_content&view=category&layout=blog&id=221&Itemid=574.

14 USAID Albania, "USAID launches the Albanian cyber-security program", 13 June 2011.

15 Carnegie Mellon Software Engineering Institute, "SEI grounds USAID–Albania effort in CERT resilience management model", 26 July 2011.

networks and offensive measures to disrupt those of the enemy.[16] The task of developing joint military doctrine for communications and electronic warfare falls on Jefatura VI (responsible for command, control, communications, information technology, and interoperability) of the armed forces.[17] The Argentine Army's Communications and Computing Systems Command includes "Computer Science Troops" who implement a comprehensive doctrine that includes "cybernetic operations" for the cyberspace battlefield.[18]

Australia

The Department of the Prime Minister and Cabinet, which assumed the responsibility from the Attorney General's Office in December 2011, coordinates Australia's cybersecurity policy. An Assistant Secretary is part of the Cyber Policy and Homeland Security Division under this department and is responsible for cyber policy and crisis management serving as the Cyber Policy Coordinator for whole-of-government cybersecurity initiatives.[19]

Australia planned to release a white paper by the end of 2012 that will lay out the state's relationship with and approach to cyberspace, likely future opportunities and challenges, and its strategic interests in cyberspace. The Cyber Security Strategy was released in 2009. It identified seven strategic priorities: developing threat awareness and response, changing civilian security culture, promoting public–private partnerships, securing government systems, pursuing international engagement, creating an effective legal framework, and building a skilled cyber workforce.[20]

The Defence Signals Directorate supports national cybersecurity initiatives such as CERT Australia and the Trusted Information Sharing Network for critical infrastructure. Australia's Cyber Security Operations Centre was

16 J.U. Ortiz, "Argentina: the challenge of information operations", *IO Sphere*, Special Edition 2008, pp. 61–62.

17 Argentine Armed Forces, "Organizacion del Estado Mayor Conjunto", www.fuerzas-armadas.mil.ar/institucional/organigrama. asp.

18 J.U. Ortiz, "Argentina: the challenge of information operations", *IO Sphere*, Special Edition 2008, p. 60.

19 N. Berkovic, "Defence on a cyber war footing", *The Australian*, 16 January 2010.

20 Australia, *Cyber Security Strategy*, 2009, p. vii.

established in 2010.[21] It is part of the Department of Defence under the Defence Signals Directorate. Its staff of 130 is comprised of specialists from the Signals Directorate, the Attorney General's Department, the Federal Police and the Australian Security Intelligence Organization.[22] The mission of the centre is to advise the government on how best to protect the country from cyber threats by disseminating information and coordinating incident response operations.[23] It is complemented by a national CERT established in 2010 that serves as a single point of contact for cybersecurity-related information.[24]

The Australian Security Intelligence Organization established a cyberinvestigations unit in March 2011. It focuses on response and intelligence regarding "state-sponsored cyber attack". Australian police worked with Indonesian police to set up the Cyber Crime Investigation Center in Jakarta in July 2011 to improve detection of cybercrime and promote bilateral coordination on cybercrime law enforcement.[25] Australia has also developed, with domestic internet service providers, a voluntary industry code on cyberspace designed to reduce botnets and malware in consumer computers.[26]

Austria

The Austrian Ministry of Defence cited cybersecurity as a major component of the defence strategy and has plans to restructure cabinet offices to include a cyber component.[27] Austria's recent national security strategy, *Shaping Security in a New Decade*, released March

21 Australian Defence Signals Directorate, "CSOC—Cyber Security Operations Centre", www.dsd.gov.au/infosec/csoc.htm.

22 N. Berkovic, "Defence on a cyber war footing", *The Australian*, 16 January 2010.

23 Australia, *Cyber Security Strategy*, 2009, p. vii.

24 CERT Australia, "About us", www.cert.gov.au/about.

25 "RI, Australian police to fight cyber crime", *Jakarta Post*, 1 July 2011.

26 Australian Department of Broadband, Communications and the Digital Economy, "Internet service providers sign up to icode", www.staysmartonline.gov.au/news/news_articles/regular/internet_service_providers_sign_up_to_icode.

27 Austrian Federal Ministry of Defence and Sport, *Weissbuch 2008*, 2009, pp. 15, 85.

2011, addresses contemporary threats, including cybersecurity.[28] The Abwehramt, Austria's military intelligence organization, cites electronic defence, including malware protection, as one of its core responsibilities.[29] It has been reported that Austria does not anticipate conventional military attacks to be a significant threat in the future and is refocusing its defence on cybersecurity as a result, and is building a cyberdefence structure consisting of 1,600 soldiers.[30]

Belarus

Belarusian military doctrine refers to cyberconflict or cyberwarfare as "information confrontation", which is seen as having the potential to be one of the main external threats facing the state. New elements of the armed forces, including new special operations forces, will be created to respond to new challenges and threats such as cyberattack. The new forces will focus on mitigating the risks from cyberspace to military security while also using it effectively as a new battlefield.[31] These units will be considered special operations units and will focus on "information security, confrontation, and counteraction".[32] The military is developing cybercapabilities for defence and early warning of cyberattack.[33] The armed forces are responsible for ensuring informational security and, in wartime, for informational confrontation and counteraction against enemy forces.[34] Belarus's agreement on cooperation with the Commonwealth of

28 G. Mader, "Austria unveils new security doctrine amid neutrality concerns", *Jane's Defence Weekly*, 8 March 2011.

29 B.S. Buckland, F. Schreier, and T.H. Winkler, *Democratic Governance and the Challenges of Cybersecurity*, Geneva Centre for the Democratic Control of Armed Forces, p. 33, http://genevasecurityforum.org/files/DCAF-GSF-cyber-Paper.pdf.

30 D. Perry, "Austria hires 1600 soldiers for 'cyber' security", *Tom's Guide*, 5 May 2011.

31 "Belarusian army to combat cyber threats", *Belarusian Telegraph Agency*, 7 December 2011.

32 Belarusian Ministry of Defence, "The military doctrine of the Republic of Belarus", chp. 2, www.mod.mil.by/doktrina_eng.html.

33 Ibid., chp. 2, paras. 7, 10.

34 Ibid., chp. 2, para. 7.

Independent States contains a provision on mutual assistance in the event of a cyberincident.[35]

Brazil

Brazil's National Defence Strategy, issued December 2008, identified cybertechnology as a strategic sector for national defence.[36] The strategy calls for the establishment of an organization dedicated to enhancing cybercapabilities in industry and the military.[37] The strategy stresses the importance of indigenous cybercapabilities and technological self-sufficiency. The technologies considered particularly important are those used in submarines and weapons systems. Brazil plans to develop indigenous cybercapabilities by building capacity in educational institutions and in the military to enhance communication among components of the armed forces.

Brazil's International Security Office is responsible for the security of public administration networks.[38] In 2010, the International Security Office announced that the Brazilian Army had created an interagency cybersecurity centre, the Centre of Cyber Defence, to protect critical military, governmental, and information infrastructure.[39] The Centre will be staffed by 140 members of the army, air force, and navy when it becomes fully operational, but the current number of staff is unclear. In 2012 the Centre received $45 million from the government for its operations.[40] The Cyber-Warfare Communications Centre is part of the Centre of Cyber Defence and has been purchasing virus and cyberattack simulators for military training purposes.[41] Brazil has established the Cyberwarfare

35 V. Golubev, "Fighting cybercrime in CIS: strategies and tactics", Computer Crime Research Center, 29 June 2005.
36 Brazilian Ministry of Defence, *National Strategy of Defence*, 2008.
37 Ibid., pp. 33–34.
38 H. Richardson, "Brazil raises cyber defence game", *[it]decisions*, 15 June 2011.
39 "Brazilian Army prepares its CDCiber, the 'Cyber Defence Center'", *Linha Defensiva*, 8 May 2012.
40 J. Hulse, "Brazil's armed forces grapple with cybersecurity challenges", *Diálogo*, 29 October 2012.
41 C. Costa, "Exército brasileiro prepara sistema de prevenção contra ataques cibernéticos", *BBC Brasil*, 10 February 2012.

Communication Centre, led by a brigadier general, in response to numerous attacks on Brazilian military networks.[42]

Brazil's regional engagement on cybersecurity recently included a conference for the Organization of American States (OAS) Inter-American Committee Against Terrorism (CICTE) on the creation and management of computer security incident response teams (CSIRTs). The Brazilian Intelligence Agency and the Department of Information Security and Cooperation contributed to educating CICTE members.[43] In 2010, Brazil and the United States signed a defence cooperation agreement. Areas of cooperation will include cybersecurity, as Brazilian personnel have participated in US Department of Defense-sponsored workshops and virtual exercises on cyberdefence.[44]

Canada

Canada issued its Cyber Security Strategy in October 2010.[45] The strategy has three pillars: securing government systems, collaborating to secure vital cyber systems outside the federal government to strengthen resiliency, including for critical infrastructure, and helping Canadians to be secure online. Public Safety Canada, the agency responsible for public safety and national security preparedness, oversees implementation of the strategy.[46] The Canadian Security Intelligence Service lists information security threats as one of its five priority areas.[47]

---

42 "Brazilian army to get cyberwarfare training and security support from Panda Security", *Security Week*, 28 September 2010.

43 OAS CICTE, "CICTE's first cybersecurity program CSIRT training course held in Brazil", www.cicte.oas.org/Rev/En/events/Cyber_Events/CSIRT%20training%20course.asp.

44 US Department of State, "U.S.–Brazil defence cooperation agreement (DCA)", 12 April 2010; US National Defense University, "NDU iCollege cyber professors: Duvall, Saunders and Hurley, are honored by the Office of the Secretary of Defense Network and Information Integration Department of Defense Chief Information Office", 22 December 2011.

45 Canada, *Canada's Cyber Security Strategy*, 2010.

46 Public Safety Canada, "Government of Canada launches Canada's cyber security strategy", 3 October 2010.

47 Canadian Security Intelligence Service, "Our priority areas", www.csis.gc.ca/prrts/index-eng.asp.

The strategy also addresses international engagement between the Department of National Defence and allied militaries on cyberdefence best practices.[48] The Canadian Armed Forces Information Management Group is responsible for the protection of the armed forces' computer and communications networks. Subsidiary organizations include the Canadian Forces Network Operation Centre as well as a centre for electronic warfare and signals intelligence. In June 2011, Canada created the Directorate of Cybernetics to build cyberwarfare capabilities for the armed forces.[49]

China

In 2012, China's State Council issued a set of new cybersecurity policy guidelines calling for intensified efforts to better detect and handle "information emergencies", reduce internet crime and better protect personal information.[50] Several ministries in China have responsibility for cybersecurity, including the Ministry of Public Security and the Ministry of Industry and Information Technology, both of which are overseen by the State Council. The Ministry of Public Security is responsible for investigating cybercrime and responding to emergencies. The Ministry of Industry and Information Technology is responsible for regulation and development, and has domestic responsibilities similar to those of the Department of Homeland Security in the United States; it sets standards, holds exercises, carries out inspections on network security, and operates the national CERT.[51]

China's State Council's Information Office issued a white paper in 2011 on national defence that built upon on previous documents.[52] It tasked the military to "maintain its security interests in space, electromagnetic space and cyber space".[53] The strategy calls for "a new type of combat capability

48 Canada, *Canada's Cyber Security Strategy*, 2010, p. 29.

49 K. Pham, "Cyber security: do your part!", *The Maple Leaf*, vol. 15, no. 2, 2012; "Canada", in *The Military Balance 2012*, International Institute for Strategic Studies, 2012, p. 53.

50 "China calls for tightened information security measures", *Xinhua*, 18 July 2012.

51 China, "Policies and practices on network security of MIIT", Asia–Pacific Economic Cooperation Workshop on Cybersecurity Policy Development in the APEC Region, 27 March 2011.

52 Information Office of the State Council of the People's Republic of China, *China's National Defense in 2010*, 2011.

53 Ibid., § II "National Defense Policy".

to win local wars in conditions of informationization". It states that the "fighting capabilities of the armed forces in conditions of informationization have been significantly raised".[54] In May 2011, the Ministry of National Defence announced that the army had established an "Online Blue Army" to improve the network security of the military forces.[55]

Colombia

The Colombian Ministry of Foreign Relations established an inter-agency working group on cyberspace in 2005. After the Ministry of Information and Communications Technology identified gaps in cybersecurity, the working group, with input from the Ministry of Foreign Relations and the Ministry of the Interior and Justice, assigned cybersecurity responsibilities to the Ministry of Defence. Colombia created a national CERT in 2009.[56] The Ministry of Defence is the lead agency in operating the CERT, although legislative, judicial, and international matters are the responsibility of the respective agencies. The Directorate for Criminal Investigations within the National Police Force, for example, now has a cybercrime investigations unit known as the Technology Investigations Group.[57]

The CERT is part of a larger national cybersecurity policy to coordinate public and private sector cyberdefence. In 2009, the Ministry of Defence called for a national cyber strategy with new tools for prevention, response, and defence. It recommended creating a joint doctrine to govern both military and police operations in cyberspace. Defence capabilities would include not only early alerts of attack on both public and private infrastructure and information, but also the ability to repel such attacks and to conduct cyberattacks against aggressors.[58] In November 2011, the Ministry of Defence ran attack simulations supported by the OAS, to test

54 Ibid., § III "Modernization of the People's Liberation Army".
55 Ye X., "PLA establishes 'Online Blue Army' to protect network security", *People's Daily Online*, 26 May 2011.
56 Colombian Ministry of National Defence, *Ciberseguridad y Ciberdefensa: Una Primera Aproximacion*, 2009.
57 G. Diniz and R. Muggah, *A Fine Balance: Mapping Cyber (In)Security in Latin America*, Igarapé Institute and the SecDec Foundation, 2012, p. 14.
58 Colombian Ministry of National Defence, *Ciberseguridad y Ciberdefensa: Una Primera Aproximacion*, 2009.

capabilities and strengthen the reaction of the state in the face of a large-scale attack.[59]

Croatia

According to the Strategic Defence Review, Croatia will be creating a Signals Unit that will be responsible for a stationary, network-information, and encryption signal systems.[60] The Security and Intelligence Agency, a part of the Ministry of Defence, ensures the government's internet security.[61] Croatia has had a national CERT since 2009.

Cuba

The Cuban government holds a monopoly on telecommunications and controls internet traffic. The Ministry of Informatics and Communications has prioritized the development of indigenous information technology to enhance cyber self-sufficiency and cybersecurity against potential external threats.[62] Cuba hopes to prevent cyberattack by developing national software and migrating state institutions to domestic, rather than imported, software and computers.[63]

Democratic People's Republic of Korea

Sources suggest that the Democratic People's Republic of Korea invests significant resources in its offensive cybercapabilities, though progress in

59 OAS, "OAS holds regional workshop in Colombia on best practices for cybersecurity and the fight against cybercrime", www.oas.org/juridico/newsletter/lc_en_19.htm.

60 Croatian Ministry of Defence, *Strategic Defence Review*, 2005, p. 27.

61 Croatian Security and Intelligence Agency, "About Security and Intelligence Agency", www.soa.hr/en/soa/about_us.

62 Cuban Ministry of the Revolutionary Armed Forces, *Doctrina Militar Cubana*, www.cubagob.cu/otras_info/minfar/doctrina/doctrina_militar.htm; and Cuba, "Preparación para la defensa", www.cubagob.cu/otras_info/minfar/colegio/prepar_defensa.htm; see also "Fighting cyber-attacks is matter of national security: Cuban minister", *Xinhua*, 25 February 2011.

63 Ibid.

this area is difficult to determine due to the lack of information on the subject.[64]

Denmark

Danish cyber strategy is defensive and focused on protecting military computer systems from exploitation or disruption.[65] Military doctrine references cyberspace as a military battlespace. The Danish Defence Agreement 2010–2014 calls for the establishment of a computer network operations unit, to promote Denmark's cyber capabilities and to protect the information technology of the armed forces from cyberattack by 2014.[66] The Defence Intelligence Service is responsible for finding and countering cyber threats and is planning to establish a cyberwarfare unit.[67] The role of the army's 3rd Electronic Warfare Company is to disrupt or exploit enemy communications.[68]

Estonia

The Cyber Security Strategy Committee was formed after Estonia was the target of the "first-ever co-ordinated cyber attack against an entire country" in May 2007, and released the Cyber Security Strategy in 2008.[69] The Committee is chaired by the Ministry of Defence in cooperation with the Ministry of Foreign Affairs, the Ministry of Internal Affairs, the Ministry of Education and Research, the Ministry of Justice, and the Ministry of Economics. The strategy seeks to decrease vulnerability in cyberspace, prevent cyberattack, and restore critical infrastructure as quickly as possible in the event of an attack. To this end, the strategy identifies the following goals: to establish a multilevel system of security measures, expand expertise in information security, institute regulatory reforms, and foster international cooperation. A unit within the Ministry of Economic Affairs

64 See "S. Korean held for selling N. Korean malware", *Asiaone News*, 4 June 2012; and "Incheon Airport cyberattack traced to Pyongyang", *Korea Joongang Daily*, 5 June 2012.

65 Denmark, *Danish Defence Agreement 2010–2014*, 2009, p. 11.

66 Ibid.

67 "Military ready to do battle in cyberspace", *Copenhagen Post Online*, 14 January 2011.

68 Danish Defence, "3. Electronic Warfare Kompagni (3 EWKMP)", www.forsvaret.dk/TGR/Organisation/3%20EWKMP/Pages/default.aspx.

69 Estonian Ministry of Defence, *Cyber Security Strategy*, 2008, p. 6.

will ensure the security of state information systems. Estonia established the Cyber Security Council within the Security Committee of the Government of the Republic to implement the strategy.[70]

The Ministry of Defence coordinates Estonia's cyberdefence.[71] The Defence League, a voluntary national defence organization, is organized and trained by the Ministry of Defence.[72] The Defence League's Cyber Unit has three main tasks: protection of the Estonian civilian internet, training IT specialists, and sharing information on cybersecurity with the public.[73] Estonia has also created the Department of Critical Infrastructure Protection, tasked to defend public and private networks at the strategic level. It conducts risk assessments, collects information on critical infrastructure, and proposes defensive measures to counter cyber threats. Projects include mapping critical infrastructure and designing contingency plans for large-scale cyberattack.[74] Estonia's focus is now shifting towards the protection of intellectual property in order to preserve economic assets and advantages over the long term.[75] To protect both critical and economic infrastructure, Estonia is building partnerships between the public and private sectors.[76]

Estonia places significant emphasis on its North Atlantic Treaty Organization (NATO) membership and international cooperation as means to augment and streamline its defence capabilities.[77] Estonia proposed the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, which was

70 Ibid., pp. 8, 29.
71 Ibid.
72 H. Kenyon, "Volunteer cyber corps to defend Estonia in wartime", *Defence Systems*, 12 January 2011.
73 Estonian Defence League, "The main tasks of the EDL CU", http://uusweb.kaitseliit.ee/en/the-main-tasks-of-the-edl-cu.
74 European Network and Information Security Agency, *Estonia Country Report*, 2011, p. 20.
75 W. Jackson, "The big target in cyber war isn't military anymore", *GCN*, 12 April 2012.
76 "Estonian president calls for greater cooperation on cyber defence", *Estonian Review*, 2 May 2012.
77 H. Laasme, "Estonia: cyber window into the future of NATO", *Joint Force Quarterly*, no. 63, 2011.

launched in 2008 to promote cooperation, information-sharing, and research in the field of cybersecurity.[78]

Fiji

Fiji has established a cybercrime unit in the police force.[79] In 2010, Fiji established the Cybersecurity Working Group led by the Cybercrimes Unit of the national police force and the Ministry of Defence. The group, based on a public–private partnership, includes government information technology departments, the Financial Intelligence Unit (which monitors illegal activities such as money laundering), licensed operators, network services providers, and banks. Fiji has addressed online financial protection as well as online customs and tax evasion issues with the establishment of the Fiji Inland Revenue and Customs Excise Authority.[80]

Finland

In March 2012, Finland's President and the Cabinet Committee on Foreign and Security Policy announced that the Security and Defence Committee will be responsible for preparing a national cybersecurity strategy to improve national preparedness.[81] Finland was planning to issue the new cybersecurity strategy by the end of 2012—however as of December 2012 it had not been released.[82] Finland also plans to improve cyberintelligence capabilities to track organized crime and terrorist threats.[83] The Ministry of Defence has drafted a national cyberdefence strategy proposal that would provide substantial investment to protect crucial military, government, and private sector networks. The plan increases funding for the military's Cyber

78 "NATO launches cyber defence center in Estonia", *Space War*, 14 May 2008, www.spacewar.com/reports/NATO_launches_cyber_defence_centre_in_Estonia_999.html.

79 Fiji Police Force, "Cyber crime", www.police.gov.fj/index.php/news/264-cyber-crime.

80 S. Tamanikaiwaimaro, "Cybersecurity in the Republic of Fiji", Diplo, www.diplomacy.edu/sites/default/files/IGCBP2010_2011_Tamanikalwalmaro.pdf.

81 Finish Government Communications Unit, "National cybersecurity strategy to be drafted in 2012", press release 94/2012, 16 March 2012.

82 Finnish Government Communications Unit, "Cyber security preparedness", press release 68/2011, 8 March 2011.

83 Prime Minister's Office of Finland, *Finnish Security and Defence Policy 2009*, 2009, p. 93.

Defence Unit to allow it to mount cyberattacks on "hostile forces" as part of a "Credible Response Platform", which is likely to deploy malware, worms, and viruses against "attackers". The initial stages of the plan could be operational by 2013.[84] Finland established a CERT, which serves as the reporting centre for information or computer security threats. It runs the national information security situation awareness system, which collects and circulates security situation reports.[85]

In September 2012, the president of Sitra, the Finnish Innovation Fund, recommended setting up a national cybersecurity centre in order to improve coordination, speed up decision-making, and develop confidence in the field. He noted that Finland does not "have the ability to respond to a large-scale cyber attack against several vitally important targets at the same time".[86]

France

The main authority for cyberdefence is the French Network and Information Security Agency, established in 2009. Its missions include detecting and reacting to cyberattack, mitigating cyber threats by supporting research and development, and providing information to government and critical infrastructure entities. It operates under the Prime Minister and is part of the General Secretariat for National Defence. In February 2011, the Agency released the official French cyber doctrine. France's four objectives in cyberspace are to become a global power in cyberdefence, guarantee information sovereignty and freedom of decision, secure critical infrastructure, and maintain privacy in cyberspace.[87]

France's white paper on defence and national security, issued in 2008, highlighted the threat of large-scale cyberattack against critical infrastructure as a prominent national security concern and defined new strategies for cyberdefence. In the document, France describes the cyber

84 G. O'Dwyer "Finland to develop cyber defence 'counterpunch'", *Defense News*, 20 October 2011.

85 Finish Communications Regulatory Authority, "CERT-FI in brief", www.cert.fi/en/index.html.

86 "Finland plans to set up national cybersecurity centre", *Helsingin Sanomat*, www.hs.fi/english/article/Finland+plans+to+set+up+national+cyber+security+centre/1329104867405.

87 French Network and Information Security Agency, *Information Systems Defence and Security: France's Strategy*, 2011.

domain as an area in which its sovereignty must be expressed fully, and states that it is pursuing a two-pronged strategy in building its defensive and its offensive capabilities.[88]

France is also developing an offensive cyberwar capability under the purview of the Joint Staff and specialized services.[89] Both the army and the air force have electronic warfare units.[90] Offensive capabilities are also being pursued by the intelligence services.[91] The Analysis and Combat Centre for Cyber Defence coordinates with the Network and Information Security Agency and other agencies to monitor military networks and respond to intrusions.[92] In addition, the Directorate for Defence Protection and Security is an intelligence agency within the Ministry of Defence that ensures the military's operational capacity by providing information about potential threats and vulnerabilities.[93] It protects against the threats of espionage, sabotage, subversion, organized crime, and terrorism. The Directorate increasingly focuses on communicating cyber threats and vulnerabilities to network operators in the military and the defence industry in order to improve cybersecurity.[94]

Georgia

The Georgian Ministry of Defence Minister's Vision 2012–2013 prioritizes the development of cybersecurity capabilities, as well as streamlining

88 European Network and Information Security Agency, *France Country Report*, 2011, p. 10.

89 France, *The French White Paper on Defence and National Security*, 2008, p. 3.

90 The army has one brigade for intelligence, surveillance, and reconnaissance that includes two electronic warfare regiments. The air force has one fleet for electronic warfare with a C-160G Gabriel for electronic surveillance; "Europe", in *The Military Balance 2011*, International Institute for Strategic Studies, 2011, pp. 104–109.

91 France, *The French White Paper on Defence and National Security*, 2008, p. 9.

92 "France", in *The Military Balance 2012*, International Institute for Strategic Studies, 2012, p. 115.

93 French Ministry of Defence, "Un service de renseignement", 22 June 2012, www.defense.gouv.fr/dpsd/la-dpsd/un-service-de-renseignement/un-service-de-renseignement.

94 French Ministry of Defence, "Direction de la Protection et de la Sécurité de la Défense", www.defense.gouv.fr/english/portail-defense.

communication and information systems.[95] Georgia's National Security Concept, approved by Parliament in December 2011, identifies cybersecurity as a key priority, emphasizing the need for rapid response and mitigation capabilities, information security, and international cooperation.[96] Georgia has been developing a National Cyber Strategy, but as of December 2012 it was not yet finalized.[97] Early reports indicated that the strategy will centre around five key objectives: research and analysis, a normative framework for new legislation, inter-agency coordination, public awareness and education, and international cooperation.[98]

As of June 2012, Georgia's parliament has been debating a draft bill on information security, which would define critical information systems as those systems whose function is essential to self-defence, economic security, preservation of state authorities, and/or public life, and which proposes an expanded system of classification to safeguard sensitive information.[99] Georgia's information security efforts are coordinated by the Data Exchange Agency, which also manages e-governance and infrastructure development efforts.[100] Georgia recently signed the Convention on Cybercrime, which entered into force in Georgia in October 2012.[101]

Germany

In March 2011, the German Federal Government released a new cybersecurity strategy. It builds on the 2009 Act to Strengthen the Security of Federal Information Technology, the 2009 Critical Infrastructure Protection Implementation Plan, and the 2005 National Plan for

95 Georgian Ministry of Defence, *Minister's Vision 2012–2013*, 2012.
96 National Security Council of Georgia, *National Security Concept of Georgia*, 2011.
97 National Security Council of Georgia, "Cybersecurity", www.nsc.gov.ge/eng/Cybersecurity.php.
98 T. Kupreishvili, "Cyber security first concept", *Netgazeti.ge*, 20 March 2012, http://netgazeti.ge/GE/97/Technology/8828.
99 N. Dzvelishvili, "Amendments to draft bill on information security", *Media.ge*, 8 May 2012, www.media.ge/en/stories/amendments_to_draft_bill.
100 Georgian Data Exchange Agency, "Cvens sesaxeb", http://dea.gov.ge/?action=page&p_id=5&lang=geo.
101 Embassy of Georgia to Turkmenistan, "Statement of the Ministry of Foreign Affairs regarding the Georgia's approval of the Council of Europe Convention on Cyber Crime", 6 June 2012, http://turkmenistan.mfa.gov.ge/index.php?lang_id=ENG&sec_id=140&info_id=15072.

Information Infrastructure Protection. The latter was Germany's first effort at a comprehensive approach to cybersecurity. Under the 2011 strategy, a National Cyber Security Council was established, headed by a state secretary from the Ministry of Interior, and a National Cyber Response Centre. The Ministry of the Interior has been the lead on cybersecurity and the Federal Office for Information Security, overseen by the ministry, is in charge of promoting the security of information technology.[102]

The National Cyber Security Council will focus on coordinating preventive and cooperative cybersecurity measures. It is composed of the Federal Chancellery and state secretaries from the Foreign Office, the Ministry of the Interior, the Ministry of Defence, the Ministry for Economics and Technology, the Ministry of Justice, the Ministry of Finance, and the Ministry of Education and Research, as well as state-level representatives. Representatives from private industry as well as academia are invited as associated members. The National Cyber Security Council is responsible for coordinating defence techniques and cyber policy.[103]

Germany's National Cyber Response Centre incorporates officials from the Federal Criminal Police Office, the Federal Police, the Customs Criminological Office, the Federal Intelligence Service, the armed forces, and critical infrastructure authorities. The Centre reports to the Federal Office for Information Security and coordinates with the Federal Office for the Protection of the Constitution and the Federal Office of Civil Protection and Disaster Assistance, (both part of the Ministry of the Interior).[104] The Centre will not develop offensive capabilities,[105] instead focusing on operational cooperation and information-sharing in areas of vulnerability protection and incident response. In August 2012, the Minister of the Interior announced the potential need for new cybersecurity legislation and that he was currently in discussions with industry.[106]

The Department of Information and Computer Network Operations of the armed forces' Strategic Reconnaissance Unit is tasked with developing cybercapabilities. In 2009, this consisted of 76 military personnel with

102 German Federal Ministry of the Interior, *Cybersecurity Strategy for Germany*, 2011, pp. 9–10.
103 Ibid.
104 Ibid., p. 8.
105 F. Knoke, "Nationales Abwehrzentrum: De Maizière preist neue Cyber-Zentrale", *Spiegel Online*, 23 February 2011.
106 "Friedrich erwägt neues IT-Sicherheitsgesetz", *DAPD*, 16 August 2012.

computer science training provided by the armed forces. The unit was reportedly designed as a specialized cyber group to be trained in offensive cyber capabilities.[107]

Greece

In 2008, Greece established the National Authority Against Electronic Attack-CERT, as part of its National Intelligence Service. The Authority is tasked with the protection of the public sector and national critical infrastructures by means both passive and active.[108] Three other publicly funded CERTs serve Greece: AUTH-CERT, GRNET-CERT, and FORTH CERT, all of them sharing responsibility for alerts, warnings and announcements, incident handling, and response and coordination.[109]

The military's investment in cyberwarfare capabilities began with the establishment of the Office of Computer Warfare in 1999. In 2004, the military established the Department of Cyber Defence, which in February 2011 was upgraded to the Directorate of Cyber Defence,[110] falling directly under the authority of the Chief of Defence.[111] The Directorate is responsible for defending against acts of cyberwarfare and to this end coordinates with the National Intelligence Service and the police. It is also responsible for the coordination of national and international cyberdefence exercises.[112] Greece conducted two rounds of national exercises in 2010

107 J. Goetz, M. Rosenbach, and A. Szandar, "War of the future: national defence in cyberspace", *Spiegel Online*, 11 February 2009.

108 Greek National Intelligence Service, "National CERT", www.nis.gr/portal/page/portal/NIS/NCERT.

109 European Network and Information Security Agency, *Greece Country Report*, 2011, p. 26.

110 J. Dimakis, "Addressing the cyber defence", *OnAlert*, 27 April 2011, www.onalert.gr/default.php?pname=Article&catid=2&art_id=5239.

111 Hellenic National Defence General Staff, "HNDGS structure", www.geetha.mil.gr/index.asp?a_id=3463.

112 J. Dimakis, "Addressing the cyber defence", *OnAlert*, 27 April 2011, www.onalert.gr/default.php?pname=Article&catid=2&art_id=5239.

and 2011,[113] and participated in the NATO Cyber Defence Exercise of 2010[114] and 2011.[115]

Hungary

Hungary's 2012 National Security Strategy identifies the need to ensure the operation of critical infrastructure networks, assess and prioritize cyber risks, raise public awareness of cyber threats, and work with international partners to protect secure information systems.[116] The National Cybersecurity Center is tasked with protecting central government systems as well as critical infrastructure from cyberattack. It is also the home of CERT-Hungary.[117] The Center is part of the Prime Minister's Office and is led by the Information Security Supervisor of the Government.[118] The Center focuses on prevention and early detection of cyberattack and is developing the technical capability to defend against such. It works with the public to raise awareness of cybersecurity, with the private sector to promote information exchange on information technology issues, and with the government to develop long-term cyber strategies. The Center represents Hungary in international forums in cybersecurity exercises and information-sharing initiatives. The Ministry of Defence is responsible for information security and has developed special classes at the Zrinyi Defence Academy to build military cybersecurity capacity.[119] During Hungary's Council of the European Union presidency in 2011, the Ministry

113 European Network and Information Security Agency, *Greece Country Report*, 2011, p. 14.

114 Hellenic National Defence General Staff, "NATO 'Cyber Defence Exercise 2010 (NCDEX-2010)'", 16 November 2010, www.geetha.mil.gr/index.asp?a_id=3461&nid=1923.

115 Hellenic National Defence General Staff, "NATO 'Cyber Coalition 2011' exercise", 18 December 2011, www.defencegreece.com/index.php/2011/12/nato-cyber-coalition-2011-exercise.

116 Hungarian Ministry of Foreign Affairs, *Magyarország Nemzeti Biztonsági Stratégiája 2012*, p. 13.

117 Hungarian National Cybersecurity Center, "About us", www.cert-hungary.hu/en/node/6.

118 European Network and Information Security Agency, *Hungary Country Report*, 2011, pp. 16, 25–26.

119 Ibid., p. 20; J. Świątkowska, "Cybersecurity in Hungary", in J. Świątkowska (ed.), *V4 Cooperation in Ensuring Cyber Security—Analysis and Recommendations*, The Kosciuszko Institute, 2012, p. 68.

of Defence hosted a European conference on cyberspace security,[120] and in October 2012 hosted the second global Cyber Security Summit, building on the first such conference held in London in November 2011.[121]

India

In November 2012, India established the National Cyber Security Coordinator as the overarching body for securing cyber systems, supported by four agencies: the National Technical Research Organisation, the National Critical Information and Infrastructure Protection Centre, the Computer Emergency Response Team, and the Ministry of Defence. The National Technical Research Organisation and the National Critical Information Infrastructure Protection Centre will be tasked with protecting critical infrastructure such as police systems, nuclear facilities, and space ground stations. The Ministry of Defence will maintain cybersecurity of the army, air force, and navy defence systems, and the National Cyber Security Coordinator will ensure that there are no overlapping functions or jurisdictions across the four cybersecurity agencies.[122] India also has a cybersecurity coordinator in the National Security Council Secretariat.[123]

The Ministry of Communications and Information Technology released a draft National Cyber Security Policy in March 2011, much of which focuses on the protection of critical infrastructure, public–private partnerships, and research and development efforts.[124] In line with the draft policy, a proposal under consideration by the National Security Council as of June 2012 would create the National Critical Information Infrastructure Protection Centre (under the National Technical Research Organisation),

120 Hungarian Presidency of the Council of the European Union, "Cyberspace could also be war theatre", 4 May 2011, www.eu2011.hu/news/cyberspace-could-also-be-war-theatre.

121 "Budapest Conference on Cyberspace", *Gov.UK*, 2 October 2012, www.gov.uk/government/news/budapest-conference-on-cyberspace.

122 B. Jain, "Final touches to cyber security infrastructure in the works", *Times of India*, 7 November 2012.

123 S. Prakash, "India to appoint a cyber security controller in National Security Council", *News Track India*, 28 August 2012.

124 Indian Ministry of Communications and Information Technology, *Discussion Draft on National Cyber Security Policy*, 26 March 2011; see also Indian Ministry of Communications and Information Technology, "Cyber security strategy", 7 March 2012, http://deity.gov.in/content/strategic-approach.

which, along with national and sector-specific CERTs, would ensure the security of the state's critical infrastructure.[125]

India set up a Joint Working Group on cybersecurity, which was to establish a testing laboratory to audit and study the vulnerabilities of critical information infrastructure and establish a multidisciplinary centre for excellence.[126] The Ministry of Defence's Defence Research and Development Organization is developing an indigenous cyberdefence system to ensure that vital sectors are safe and secure. As of May 2012, the project was reportedly about 50 per cent complete.[127] The Defence Intelligence Agency and the National Technical Intelligence Communication Centre are creating a joint team to alert the government to potential cybervulnerabilities.[128]

Multiple organizations within the Ministry of Defence are responsible for cybersecurity. The Defence Information Warfare Agency coordinates information warfare responses.[129] In 2005, the Indian Army created the Cyber Security Establishment to secure networks at the division level and to conduct security audits.[130] The army also established the Cyber Security Laboratory at the Military College of Telecommunications Engineering in April 2010.[131] In July 2012, the Indian Navy announced the formation of a new cadre of information technology officers dedicated to managing, administering, and protecting critical networks. The navy has said that the officers will not engage in offensive operations.[132] The National Technical Research Organisation, along with the Defence Intelligence Agency, is responsible for developing offensive cybercapabilities. India's National Security Advisory Board has recommended the creation of

125 J. Joseph, "India to add muscle to its cyber arsenal", *Times of India*, 11 June 2012.
126 "Cyber security panel high on India's agenda", *Times of India*, 16 October 2012.
127 "India developing cyber defense program", *Xinhua*, 4 May 2012.
128 H. Singh and J. Thomas Philip, "Spy game: India readies cyber army to hack into hostile nations' computer systems", *Economic Times*, 6 August 2010.
129 See V. Anand, "Integrating the Indian military: retrospect and prospect", *Journal of Defence Studies*, vol. 2, no. 2, 2008, p. 37.
130 R. Pandit, "Army gearing up for cyber warfare", *Times of India*, 7 July 2005.
131 "Army sets up cybersecurity lab", *Governance Now*, 6 April 2010, www.governancenow.com/news/regular-story/army-sets-cyber-security-lab.
132 "Indian Navy to have information technology cadre", *Economic Times*, 12 July 2012.

central cybersecurity command modelled on the United States Cyber Command.[133]

Indonesia

In March 2012, Indonesia's Deputy Defence Minister announced plans for the creation of a cyberdefence unit to secure networks related to defence and military infrastructures.[134] Indonesia has drafted cyber legislation.[135] A 2007 decree by the Ministry of Communication and Information Technology tasked Indonesia's Security Incident Response Team on Internet Infrastructure / Coordination Center with a wide range of cybersecurity functions, including advising on major cyber threats, improving national cyberdefence (especially in critical infrastructure), and supporting law enforcement with regard to cybercrime.[136]

Islamic Republic of Iran

The Islamic Republic of Iran has put significant effort into developing cybercapabilities. In March 2012, a decree was issued establishing the Supreme Council of Cyberspace, to include heads of intelligence, militia, security, media, and the Revolutionary Guard Corps.[137] The Council is tasked with the coordination of national cyberwarfare and information security and may play a role in the effort to develop a national internet.[138]

---

133 Indian Ministry of Communications and Information Technology, *Discussion Draft on National Cyber Security Policy*, 26 March 2011; see also Indian Ministry of Communications and Information Technology, "Cyber security strategy", 7 March 2012, http://deity.gov.in/content/strategic-approach.

134 J. Grevatt, "Indonesia to establish cyber-defence unit", *IHS Jane's*, 30 November 2012.

135 "Cybercrime legislation of Indonesia", presentation by Ashwin Sasongko, Director General of ICT Application, Indonesian Ministry of Communication and Information Technology, at the Octopus Interface Conference, Strasbourg, 23–25 March 2010, http://unpan1.un.org/intradoc/groups/public/documents/UNGC/UNPAN040467.pdf.

136 The Decree of the Minister of Communication and Information Technology number 26/PER/M.KOMINFO/5/2007 on Securing the Making Use of Internet Protocol Based Telecommunication Network.

137 "Iran's cyber police to keep checks on internet use", *Gulf News*, 24 March 2012.

138 See www.leader.ir/langs/fa/?p=contentShow&id=9213; "The Islamic Republic takes another decisive step towards controlling cyberspace in Iran", *Iran Politik*,

The acting commander of the Basiji, a paramilitary force, announced that state's cyber army is made up of some 120,000 university teachers, students, and clerics. The Islamic Republic of Iran announced in June 2011 that it plans to establish a cyber command for the armed forces to defend against cyberattack and to centralize operations. Iranian officials state that the cybercommand will be defensive and that it will be primarily concerned with thwarting efforts to incite dissent within the country.[139] Iranian cyber capabilities are coordinated within the military by the Passive Defence Organization.[140] The Islamic Revolutionary Guard Corps also has a cyberwarfare unit. In 2010, a military commander described this as the second largest cyber army in the world.[141] The Iranian Cyber Police Unit, launched in 2011, is mainly used to police social media websites.[142]

Israel

In May 2011, Israel launched its National Cyber Defence Initiative, creating the National Cybernetic Taskforce. The Taskforce's recommendations led to the establishment of the National Cyber Directorate in the Prime Minister's Office. The Directorate's task is to ensure inter-agency coordination and expand cybersecurity in critical infrastructure and industry.[143] The Directorate is developing a national cyberdefence concept and appropriate regulations, and promoting international cooperation.[144]

Civilian cybersecurity is handled by the National Information Security Authority within the Israel Security Agency, established in 2002 with the goal of securing critical infrastructure, formulating information security strategies, and publishing threat scenarios. It has authority over several major operators of critical infrastructure, including electricity providers,

28 March 2012.

139 "Iran's armed forces to launch 'cyber command': commander", *Xinhua*, 15 June 2011.

140 "Iran mobilises cyber hacking army", *Security Technology News*, 15 March 2011.

141 "Iranian cyber army second-largest in the world, claims Iranian commander", *The New New Internet*, 21 May 2010.

142 "Iranian cyber police on web patrol", *Euronews*, 24 January 2011.

143 Israeli Prime Minister's Office, "Cabinet approves the creation of the National Cyber Directorate", 7 August 2011.

144 Israeli Ministry of Foreign Affairs, "National Cyber Bureau work plan presented", 7 June 2012.

banks, and government entities,[145] and is empowered to levy sanctions against organizations in violation of its directives. It has limited power, however, over other government entities such as the Israeli Defense Forces, issuing prescriptive guidelines but lacking formal oversight.[146] In November 2012, Israel announced that it is creating a dual cybersecurity programme called MASAD, which will promote research and development for both civilian and defence purposes.[147]

Military-oriented operations are split between the Israel Defence Forces' Unit 8200—which deals with signals intelligence and encryption—and the C4I Corps. Unit 8200 is staffed by military conscripts and officers, and it focuses on three areas of cybersecurity: intelligence gathering, defence, and attack.[148] The C4I Corps is responsible for communication and organizing cyberdefence capabilities, with teams that test firewalls and encryption.[149] In 2009, to improve cooperation between Unit 8200 and C4I, a senior intelligence officer was assigned to the C4I's Centre for Encryption and Information Security with responsibility for assessing technological advances in cybercapabilities among Israel's adversaries.[150] Senior military officials have said that cyberwarfare fits well with Israel's military doctrine, and that it gives small states abilities once only available to superpowers.[151]

Italy

Italy's 2010 Annual Report on the Information System for the Security of the Republic identified cybersecurity as a growing challenge to national security.[152] In June 2012, Italy held the state's first national cybersecurity exercise, involving the Council of Ministers, and the Ministries of Defence, Public Administration, and Public Safety, to test the security

145 See www.ynet.co.il/articles/1,7340,L-3183366,00.html.
146 L. Tabansky, "Critical infrastructure protection against cyber threats", *Military and Strategic Affairs*, vol. 3, no. 2, p. 72.
147 C. Ya'ar, "Gov't establishes dual cyber security program", *Arutz Sheva*, 1 November 2012.
148 A. Oren, "IDF dependence on technology spawns whole new battlefield", *Haaretz*, 3 January 2010.
149 Ibid.
150 Ibid.
151 Ibid.
152 F. Di Camillo, V. Miranda, and S. Felician, *Cyber-Security: Europe e Italia*, *Osservatorio di politica internazionale*, no. 32, 2011.

services' response to a series of simulated attacks by cyber criminals.[153] The Ministers of Communications, Justice, and Internal Affairs created a permanent observer group for the security and protection of networks and communications. The Data Protection Authority and the police collaborate on a regular basis to stop and prevent criminal activities involving spam and spyware. Italy does have a CERT; however it has "insufficient funds to operate on a global scale".[154]

The Italian military has an electronic warfare unit responsible for intelligence, surveillance, target acquisition, and reconnaissance.[155] Other elements monitoring cybersecurity include the Defence Innovation Centre and the Division for Information Security of the Defence Staff. Additionally, the Telematics Section of the Carabinieri was established to combat cybercrime and terrorism.[156] Italy participated in a seven-country exercise organized by the European Network and Information Security Agency in June 2012 to test national response mechanisms and to improve cross-border coordination,[157] and it is a founding member of the NATO Cooperative Cyber Defence Centre of Excellence.[158] Italy is a signatory of the Convention on Cybercrime and has enacted or amended legislation to provide a legal framework for combating cybercrime.[159]

Japan

Japan is beginning to create new organizations and to fund research on cybercapabilities and hopes to issue a comprehensive national cybersecurity strategy in 2013. The National Information Security Center and the Information Security Policy Council, both established in 2005 in

153 Italian Ministry of Economic Development, "Cyber Italy 2012: prima esercitazione nazionale sulla sicurezza informatica", 19 June 2012.

154 B. Grauman, *Cyber-Security: The Vexed Question of Global Rules*, Security and Defence Agenda, 2012, pp. 67–68.

155 "Europe", in *The Military Balance 2011*, International Institute for Strategic Studies, 2011.

156 European Network and Information Security Agency, *Italy Country Report*, 2011, pp. 9–10.

157 European Network and Information Security Agency, "Exercises boost cooperation", 13 June 2012.

158 "NATO launches cyber defence centre in Estonia", *Agence France-Presse*, 14 May 2008.

159 European Network and Information Security Agency, *Italy Country Report*, 2011, p. 9.

the Cabinet Office, are responsible for national security and emergency response systems, including guarding against cyberattack. The Center drafts standards, formulates recommendation, and reports to the Cabinet Secretariat.[160] It is supported by the Government Security Operation Coordination team, which became operational in 2008. The team monitors government information systems and implements the Center's directives. Japan's 2009 National Strategy on Information Security indicates that all government agencies must assist the team in improving cyber defences.[161]

Japan's Ministry of Defence plans to create a 100-member cyberdefence unit in 2013.[162] Currently, the Japan Self-Defense Force has four units with 360 members responsible for protecting military computer systems. The Command, Control, Communications, and Computer Systems Command, established in 2008, will develop cyberdefence capabilities at the national level. The Command's Cyberspace Defence Unit will integrate cyberdefence into the military, provide coordination and technical and training assistance, and research cyberwarfare options. Japan's 2010 defence white paper highlighted cyber activity as a new development in warfare and described trends in cyberwarfare capabilities.[163] In June 2011, Japan and the United States announced a bilateral strategic policy dialogue on cybersecurity issues.[164]

Japan's Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade, and Industry established the Cyber Clean Center to study botnets, analyse their occurrence, and develop countermeasures. Internet service providers and security vendors assist with the research.[165] In October 2011, because of attacks on Mitsubishi and other Japanese corporations, the Ministry of Economy, Trade, and Industry established the Japan Cyber Security Information Sharing Partnership to facilitate

160 Japanese National Information Security Policy Council, *The First National Strategy on Information Security*, 2006, p. 1.

161 Japanese National Information Security Policy Council, *The Second National Strategy on Information Security*, 2009, p. 54.

162 K. Mizokami, "New Japan Self Defense Force initiatives on amphibious warfare, Global Hawk, cyber-terrorism", *Japan Security Watch*, 28 August 2012.

163 Japanese Ministry of Defence, *Defence of Japan 2010*, part I, chp. 1, § 3.

164 M. Weisgerber, "Japan, U.S. to expand missile defense, cyber cooperation", *Defense News*, 21 June 2011.

165 M. Lasar, "Japan has national botnet warriors; why don't we?", *Ars Technica*, 21 October 2010.

information-sharing among manufacturers of core technology[166] and various public and private cybersecurity organizations.[167]

Kazakhstan

Kazakhstan's 2011 Military Doctrine identifies cyberterrorism and the use of information technologies and psychological warfare to interfere in Kazakhstan's internal affairs as threats facing the country.[168] The Ministry of Communication and Information controls much of the country's IT infrastructure.[169] In 2009, Kazakhstan established a CERT in the Ministry of Communications and Information to monitor and protect the .kz domain. Additionally, the Kazakhstan Committee of National Security has created the Computer Crime Unit.[170] Kazakhstan proposed creating a cyber police agency within the Shanghai Cooperation Organization and has participated in Collective Security Treaty Organization discussions on efforts to combat cybercrime.[171] Kazakhstan's civil nuclear cooperation agreement with India also included a memorandum of understanding between the states' CERTs supporting coordination in the event of a cyberattack, including mutual response to cyberincidents, the exchange of information on threats and attacks, and the exchange of human resources.[172] It also meets with foreign CERT programmes to improve effectiveness.[173]

---

166 Namely IHI, Kawasaki Heavy Industry, Toshiba, NEC, Hitachi, Fuji Heavy Industry, Fujitsu, and Mitsubishi Heavy Industry.

167 See www.ipa.go.jp/security/J-CSIP/documents/presentation1.pdf.

168 Ministry of Defence of the Republic of Kazakhstan, "Military doctrine", http://mod.gov.kz/mod-en/index.php/2009-06-26-02-25-27.

169 See "Kazakhstan", in S. Kelly and S. Cook (eds.), *Freedom on the Net 2011: A Global Assessment of Internet and Digital Media*, Freedom House, 2011, pp. 214–223.

170 M. Laruelle, "Cybersecurity in Central Asia: real issues, false excuse?", *Central Asia Policy Brief*, no. 2, Elliot School of International Affairs, 2012, p. 3.

171 R. Weitz, "Astana backs wider SCO regional role", *Eurasia Daily Monitor*, vol. 9, no. 120, 25 June 2012; M. Domnitskaya, "CSTO to combat cyber crime", *The Voice of Russia*, 16 August 2011.

172 "India, Kazakhstan sign seven bilateral agreements (update)", *Asian News International*, 16 April 2011.

173 Kazakhstan CERT, "KZ-CERT", http://kz-cert.kz/en.

Lithuania

In 2011, Lithuania published its cybersecurity strategy, the Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019, which sets objectives for securing state-owned information resources, efficient functioning of critical information infrastructure, and cybersecurity for all Lithuanian internet users. Additionally, the Programme identifies the required tasks for achieving these objectives and divides responsibility for these tasks among numerous ministries. The Programme also sets a 2015 deadline for a Cyber Defence Plan to address defence institutions' critical information infrastructure, to be followed by a National Cyber Defence Plan in 2019, covering critical information infrastructure and national information resources. Lithuania has, according to its Prime Minister, established a national cyber coordinator position. Lithuania continues to develop cybersecurity laws.[174] Lithuania's military doctrine classifies cyberspace as a warfighting environment and identifies "massive cyberattack" as a potential threat to the country.[175]

Malaysia

Malaysia has established national policies and organizations to promote cybersecurity. The National Cyber Crisis Committee, operating under the National Security Council, provides policy direction for cybersecurity.[176] Additionally, the National Cyber-Security Policy seeks to address threats to critical national information infrastructure by defining 10 critical sectors and eight policy thrusts to ensure protection.[177] The Ministry of Defence implements information technology security policy to protect government and business from cyberattack. Its missions include ensuring the safety of networks and preventing cyberincidents from having harmful economic

174 Lithuania, *Programme for the Development of Electronic Information Security (Cyber-Security) for 2011–2019*, 29 June 2011, pp. 2–4 and annex.

175 Chief of Defence of the Republic of Lithuania, *Lithuanian Military Doctrine*, 10 March 2010, pp. 21, 50.

176 Remarks of Ahmad Zahid Hamidi at the 11th International Institute for Strategic Studies Asia Security Summit, 3 June 2012, www.iiss.org/conferences/the-shangri-la-dialogue/shangri-la-dialogue-2012/speeches/fourth-plenary-session/ahmad-zahid-hamidi.

177 See NITC Malaysia, "National Cyber-Security Policy (NCSP)", http://nitc.mosti.gov.my/nitc_beta/index.php/national-ict-policies/national-cyber-security-policy-ncsp.

effects. CyberSecurity Malaysia, part of the Ministry of Science, Technology, and Innovation, coordinates national cybersecurity policy implementation. Cybersecurity Malaysia is also involved in cyber emergency response, digital forensics, and law enforcement to combat cybercrime, and provides a help centre for internet users, a training centre for professionals, and public alerts on cyber threats.[178] To support these efforts, CyberSecurity Malaysia hosts annual Cyber Crisis Exercises to assess national capabilities to withstand a cyberattack.[179] Malaysia continues to develop new cybersecurity laws in response to increased attacks against government websites.[180] Malaysia's CERT, formed in 1997, addresses the computer security concerns of internet users and cites its goal as the reduction of successful attacks and lowering the risk of damage from cyberattack.[181]

Myanmar

Myanmar established the Defence Services Computer Directorate in 1990, which was later renamed Military Affairs Security and given the mission to work on network-centric warfare, cybercapabilities and electronic warfare.[182] Military Affairs Security reportedly has received assistance from China.[183]

Netherlands

In 2012, the Netherlands Ministry of Defence released its Defence Cyber Strategy. There are six specific priorities addressed in the Strategy: a

178 CyberSecurity Malaysia, "Corporate information", www.cybersecurity.my/en/about_us/brief_detail/main/detail/729/index.html?mytabsmenu=0.

179 Malaysian National Security Council, "Cyber security awareness among Malaysians", www.mkn.gov.my/mkn/default/article_e.php?mod=4&fokus=17.

180 NITC Malaysia, "Cyberlaws in Malaysia", http://nitc.mosti.gov.my/nitc_beta/index.php/national-ict-policies/cyberlaws-in-malaysia.

181 Malaysia Computer Emergency Response Team, "About us", www.mycert.org.my/en/about/about_us/main/detail/344/index.html.

182 A. Zaw, "Than Shwe's 'The Art of War'", *The Irrawaddy*, 1 April 2009.

183 B. McCartan, "Myanmar on the cyber-offensive", *Asia Times*, 1 October 2008; International Crisis Group, *Burma/Myanmar: How Strong is the Military Regime?*, ICG Asia Report no. 11, 21 December 2000; W. Ashton, "Burma receives advances from its silent suitors in Singapore", *Jane's Intelligence Review*, 1 March 1998; D.S. Mathieson, "Book review: Strength and Dishonor: Building the Tatmadaw by Maung Aung Myoe", *Asia Times*, 4 July 2009.

comprehensive approach, enhancing defensive capabilities, developing offensive military capabilities, improving information-gathering and security skills, improving and encouraging innovation, and continuing to foster and develop domestic and international cooperation efforts. The Strategy describes the offensive capabilities as a "force multiplier" for increasing military effectiveness and preserving an "active defence", while recognizing the reality that the use of cyber techniques as a military tool is still in its infancy.[184]

The National Cyber Security Centre was created on 1 January 2012 with the purpose of providing expertise and advice, and monitoring threats and managing crises, and encompasses the previously existing GOVCERT.NL.[185] The Centre has published a security checklist for supervisory control and data acquisition for industrial control systems, and the *Cyber Security Assessment Netherlands* report, which assesses the short-term goals and needs of the government regarding cybersecurity.[186]

The Netherlands issued the National Cyber Security Strategy in 2011. The Strategy has five components: linking and reinforcing initiatives, promoting individual responsibility, creating public–private partnerships, pursing international cooperation, and striking a balance between self-regulation and legislation. It calls for annual trend reports in cybercrime and digital security, and states that a national information and communications technology "Crisis Plan" will be published in mid-2011, although as of December 2012 the report had not been publicly released. The Strategy places heavy emphasis on regulating cybercrime and launched an initiative to ensure that all information and communications technology parties report data loss, theft, or misuse.[187] There will also be a Cyber Education and Training Centre to research cyberdefence and to develop the human capital necessary to bolster a growing digital economy.[188]

---

184 Dutch Ministry of Defence, *Defensie Cyber Strategie*, 27 June 2012, pp. 4, 6, 11.

185 Dutch National Cyber Security Centre, "Services", www.ncsc.nl/english/services.

186 Dutch National Cyber Security Centre, *Cyber Security Assessment Netherlands*, 2011; Dutch National Cyber Security Centre, *Checklist Security of ICS/SCADA Systems*, 2012.

187 Dutch Ministry of Security and Justice, *The National Cybersecurity Strategy: Success Through Cooperation*, 2011.

188 Ibid.

The Ministry of the Interior coordinates interdepartmental cybersecurity among various civilian and military units responsible for cyber issues; the Ministry of Defence will cooperate on cyberdefence.[189] The Netherlands Ministry of Defence plans to invest in the development of cyberwarfare capabilities despite budget cuts in other areas. The Netherlands does not have a specific unit for cyberwarfare, but Netherlands military officials say that this may change in the future.[190] The Netherlands has a memorandum of understanding with Luxembourg and Belgium on cooperation in cybersecurity, including information- and expertise-sharing, cooperation on best practices, and the development of public–private partnerships.[191]

According to the 2011 annual report of the Military Intelligence and Security Service, the military established The Defence Taskforce Cyber in January 2012 in order to gather intelligence on cyber activities and threats, as well as to create closer coordination with the Sigint-Cyber Unit.[192] The National Coordinator for Counter-Terrorism has expanded its mission to include a cyber component, specifically in testing the vulnerability of internet applications against cyberattack.[193]

Norway

Norway completed the drafting stage of a National Cyber Defence Strategy in 2010.[194] The Strategy proposes 22 measures to strengthen Norway's ability to prevent and manage cyber events. The main objectives are the

189 The army, as part of its intelligence signals and reconnaissance forces, has one battalion that contains a company specializing in electronic warfare; see D. Eijndhoven, "Dutch government to design cyber defense doctrine", *Infosec Island*, 27 February 2011.

190 R. Ackerman, "Funding constraints help define Dutch military networks", *Signal Online*, May 2011.

191 "Benelux sign memorandum of understanding on cybersecurity", *European Urban Knowledge Network*, 12 April 2011.

192 Dutch Military Intelligence and Security Service, *Annual Report MIVD 2011*, 2012, pp. 49–50, 57, www.defensie.nl/_system/handlers/generaldownloadHandler.ashx?filename=/media/jaarverslag_mivd_2011_eng_tcm46-197882.pdf; D. Eijndhoven, "Dutch military intelligence dives into cyber", Argent Consulting, 21 May 2012.

193 Dutch Ministry of Security and Justice, *The National Cybersecurity Strategy: Success Through Cooperation*, 2011, p. 12.

194 G. O'Dwyer, "Norway drafts cyber defense initiative", *Defence News*, 27 January 2010.

following: to establish a common situational overview and understanding of the cyber threat, secure information and communications systems, raise awareness and education about the cyber threat, strengthen the ability to detect and manage incidents, combat and investigate incidents, and strengthen the coordination of cybersecurity.[195] The National Security Authority will receive a budget increase of 30 per cent in 2013. The Authority reports to both the Ministries of Defence and Justice and is responsible for preparing preventive and protective digital security measures. Norway's CERT is a department of the National Security Authority.[196]

The Long-Term Plan for Defence,[197] released in March 2012, states that the Ministry of Defence is to strengthen capacities in cyberdefence and intelligence.[198] In September 2012, the armed forces established the Cyber Defence Force as a "separate entity tasked with securing the Armed Forces against cyber threats".[199]

Poland

Responsibility for cybersecurity in Poland is divided between the Ministry of Administration and Digitization and the Internal Security Service.[200] The Ministry of National Defence also has significant cyber responsibilities for military networks. In 2010, Poland developed the Governmental Action Plan for Cybersecurity 2011–2016. It called for the creation of an Interministerial Coordination Team for Protection of Cyberspace and a Government Representative for Protection of Cyberspace, as well as representatives from other public and private entities.[201] The Ministry of Administration and Digitization now has responsibility and has set up a

195 See www.regjeringen.no/nb/dep/fd/dok/hoeringer/hoeringsdok/2010/forslag-til-strategi-for-cybersikkerhet/Horingsnotat.html?id=599898.

196 G. O'Dwyer, "Norway drafts cyber defense initiative", *Defence News*, 27 January 2010.

197 Norwegian Ministry of Defence, "The Norwegian Long-term Defence Plan—summary", 17 April 2012.

198 Ibid.

199 J. Benitez, "Norway increasing its 2013 defense budget, including 30% boost for cyber security", Atlantic Council, 8 October, 2012.

200 J. Świątkowska (ed.), *V4 Cooperation in Ensuring Cybersecurity—Analysis and Recommendations*, The Kosciuszko Institute, 2012.

201 J. Świątkowska, "Cyber security in Poland", in ibid.

task force for implementation.[202] The government CERT has responsibilities for both public and private networks, including critical infrastructure.[203] The Internal Security Service manages the CERT.[204]

The Ministry of National Defence's *Vision of the Polish Armed Forces 2030* gives greater emphasis to cybersecurity, and protecting information resources and the energy sector.[205] The 2009 Defence Strategy identifies cyberattack as a dangerous threat.[206] Poland will create an "Independent Information Force" in the armed forces to integrate electronic intelligence, psychological operations, and cyberoffensive and defensive actions. Poland's NATO partnership is an important element of its cyberdefence strategy. The Computer Incident Response System is responsible for cybersecurity in the Ministry of National Defence. The System is supervised by the Director of the Information Technology and Telecommunication Department, who coordinates cybersecurity functions and is supported by the Ministerial Centre for Network Security and ICT [information and communications technology] Services Management. In 2011, Poland signed an agreement with the NATO Consultation, Command, and Control Agency that would facilitate the development of new technologies to counter cyber threats.[207]

Republic of Korea

The Korea Communications Commission announced a national cybersecurity strategy in August 2011, developed through the joint

202 Permanent Mission of the Republic of Poland to the United Nations Office and International Organisations in Vienna, "Information on the Code of Conduct on Political-Military Aspects of Security in 2011", p. 12, www.osce.org/fsc/89726.

203 Polish Governmental Computer Security Incident Response Team, "About us", http://cert.gov.pl/portal/cee/38/77/About_us.html.

204 J. Świątkowska, "Cyber security in Poland", in J. Świątkowska (ed.), *V4 Cooperation in Ensuring Cybersecurity—Analysis and Recommendations*, The Kosciuszko Institute, 2012, p. 41.

205 Polish Ministry of National Defence, *Vision of the Polish Armed Forces 2030*, 2008, p. 14.

206 Polish Ministry of National Defence, *Defence Strategy of the Republic of Poland*, 2009, p. 5.

207 Polish Ministry of National Defence, "Poland signs advanced technology agreement with NATO C3 Agency", 24 February 2011.

effort of 15 government agencies.[208] Cyberspace will be considered an operational domain, such as land, air, and sea, which thus needs a state-level defence system.[209] The strategy will focus on defence, i.e., prevention and detection of, and response to cyberattack.[210] The National Cyber Security Center is responsible for identifying, preventing, and responding to cyberattack. It works with the private and military sectors to prevent cyberattack, analyse vulnerabilities, and coordinate cyber emergency response activities.[211]

The 2008 defence white paper identified cybersecurity as an essential component of national defence.[212] The 2010 white paper outlines cyberattack as one of several non-traditional security threats.[213] CERTs have been created at the corps level to oversee the Defence Information Systems.[214] The white paper also details the security measures taken by the Ministry of National Defence to protect the Defence Information Network as well as the Battlefield Management System.[215]

The Ministry of National Defence established the Cyber War Centre in January 2010. Its primary aim is to increase the security of government and financial information networks.[216] The Ministry of National Defence has also created an independent Cyber Warfare Command responsible for defensive and offensive operations in cyberspace,[217] and employing over 200 personnel.[218]

According to the Korea Communications Commission, the National Intelligence Service will play the lead role in cyber issues. The Commission,

208 A. Valdez, "South Korea outlines cyber security strategy", *FutureGov*, 13 August 2011.
209 Ibid.
210 Ibid.
211 Korean National Cybersecurity Center, "NCSC information", http://service1.nis.go.kr/eng/intro/NCSCInfo.jsp.
212 Ministry of National Defence of the Republic of Korea, *Defence White Paper 2008*, 2008, pp. 192–219, 222.
213 Ministry of National Defence of the Republic of Korea, *Defence White Paper 2010*, 2010, pp. 8–10.
214 Ibid., pp. 164–65.
215 Ibid.
216 Ibid.
217 "Cyber security Is vital for national defence", *Chosunilbo*, 2 November 2009.
218 "The Republic of Korea", in *The Military Balance 2012*, International Institute for Strategic Studies, 2012, p. 261.

along with the Ministries of National Defence and Government Administration and Home Affairs, will be tasked respectively with private sector security, national defence, and protecting the safety of the government's computer systems.[219] Currently, more than 95 per cent of the country's households have access to the Internet. The new strategy would require encryption and data back-up in the public and private sectors, as well as other security precautions.[220] The Korea Advanced Institute of Science and Technology established the Cyber Security Research Center, which has assisted in detecting and defending against cyberattack.[221] The Republic of Korea also plans to develop offensive and defensive cyberwarfare weapons, and increase manpower in the Cyber Warfare Command; the defence plan aims to boost the number of personnel to 1,000.[222]

Russian Federation

In July 2012, the Russian Federation's Security Council released a national policy for fighting cybercrime and the creation of a national system to detect and prevent cyberattack. Responsibility for policy, which aims to secure the country's networks by 2020, was given to the Federal Security Service.[223]

In January 2012, the Russian Federation's Defence Ministry published its "Conceptual Views Regarding the Activity of the Armed Forces of the Russian Federation in the Information Space". The strategy discusses the principles of information security and different measures to control for interference in information systems. Section 3 of the strategy assesses different rules for deterrence and conflict prevention and resolution.[224] In March 2012, the Russian Federation announced that it was considering establishing a cybersecurity command to secure information for the armed

219 "S. Korea charts out national cyber security strategy", *Antara News*, 9 August 2011.

220 "South Korea develops cyber security strategy", *InTelligence*, 28 August 2011.

221 Shin Ji-hye, "Joo Dae-joon, pioneer in Korean cyber security", *Korea Industry and Technology Times*, 21 May 2012.

222 "South to upgrade defense against North cyberattacks", *Korea JoongAng Daily*, 30 August 2012.

223 "Russia rolls out state cyber security policy", *Cnews*, 12 July 2012.

224 See Atlantic Organization for Security, "Russia's cyber strategy published", 15 April 2012.

forces. In addition, the government has drafted a bill to create an advanced military research agency for cybersecurity.[225]

The Military Doctrine of 2010 discusses the use of political and informational instruments to protect national interests and those of allies. The Doctrine defines the characteristic features of modern military conflict as including the integrated use of military force and non-military capabilities, and a greater role for information warfare.[226]

Singapore

The National Infocomm Security Committee formulates cyber policy and security strategy. The Singapore Infocomm Technology Security Authority oversees network security. This agency operates under the Internal Security Department of the Ministry of Home Affairs.[227] Singapore announced in 2011 that it will create the National Cybersecurity Centre to combat cyber threats. The Singapore Infocomm Technology Security Authority will head the Centre. The Centre is planned to become fully operational in 2013–2014; phase one, the establishment of a monitoring system for critical infrastructure and emergency services sectors, was accomplished in 2011.[228] The Authority also has a programme to recruit information technology professionals to serve as cyber defenders.[229] In November 2012, Singapore amended its Computer Misuse Act to help the government counter cyberattack. The amendment gives the government the ability to order an organization to act against a cyberattack before the attack is carried out.[230] The Minister of State for Defence and Education

225 "Russia considering cyber-security command", *RIA Novosti*, 21 March 2012.

226 See School of Russian and Asian Studies, "The military doctrine of the Russian Federation approved by Russian Federation presidential edict on 5 February 2010", 20 February 2010, www.sras.org/military_doctrine_russian_federation_2010.

227 S. Lemon, "Singapore to form national cyber-security agency", *IDG News Service*, 30 September 2009.

228 I. Saifulbahri, "Singapore to set up National Cyber Security Centre", *Channel NewsAsia*, 21 September 2011.

229 T. Thia, "Singapore seeks volunteers to beef up cyberdefense", *ZDNet*, 28 September 2010.

230 E. Phneah, "Singapore amends law to counter cyberattacks", *ZDNet*, 12 November 2012.

announced in July 2012 that the Ministry of Defence is also setting up a new cyberdefence training centre to help build cybersecurity expertise.[231]

Slovakia

Slovakia has distributed responsibility for cybersecurity among a number of agencies, including the Ministry of Finance (whose Division of Legislation, Standards, and Security of Information Systems is tasked with protecting critical infrastructure), Ministry of Interior, Ministry of Defence, the Personal Data Protection Office, the Slovak National Accreditation Service, and the National Security Authority. The Authority oversees cyberdefence and leads an intersectoral working group established to coordinate cyberdefence activities. The 2008 National Strategy for Information Security defined prevention, readiness, and sustainability as three strategic goals for cybersecurity.[232] The Defence Strategy of the Slovak Republic, issued in 2005, identifies the cyber domain as a key area in a changing security environment.[233] Slovakia routinely participates in NATO cybersecurity exercises (under the guidance of the National Security Authority).[234]

South Africa

The South African Cabinet approved a National Cyber Security Policy Framework in March 2012 to fight national security threats in cyberspace. The Framework named the State Security Agency the primary government institution for the development, implementation, and coordination of cybersecurity initiatives in place of the Department of Communication, which formerly led cybersecurity efforts.[235] The Agency uses a government-

231 Singaporean Ministry of Defence, "Speech by Minister of State for Defence and Education, Lawrence Wong, at the Cyber Defenders Discovery Camp Closing Ceremony, Science Centre Singapore", 7 June 2012.

232 European Network and Information Security Agency, *Slovakia Country Report*, 2011, pp. 5–6.

233 National Council of the Slovak Republic, *The Defence Strategy of the Slovak Republic*, 2005, pp. 3–4.

234 J. Vyskoč, "Cyber security in Slovakia", in J. Świątkowska (ed.), *V4 Cooperation in Ensuring Cybersecurity—Analysis and Recommendations*, The Kosciuszko Institute, 2012, pp. 52–55.

235 South African Government Information, "Statement on the approval by Cabinet of the Cyber Security Policy Framework for South Africa", 11 March 2012.

owned company, Electronic Communications Security (Pty) Ltd, to provide cybersecurity for government agencies. South Africa's cybercrime law, the Electronic Communications and Transactions Act, penalizes hacking, electronic fraud and extortion, denial of service attacks, and spam. The Act was modelled on the Convention on Cybercrime, which South Africa has signed.[236]

The Ministry of Defence's cyber responsibilities include support for civilian agencies, defence of military networks, deterrence, and offensive missions to enhance information superiority.[237]

Spain

Spain's 2011 Security Strategy identifies cyber threats as one of the eight primary risks the country faces, noting that cyberspace represents a new and unique domain. The Strategy proposes strengthening domestic cybersecurity laws, creating public–private partnerships, enhancing European and global cybersecurity cooperation, and developing a cyber security strategy.[238] The Ministry of Defence oversees cybersecurity for the military.[239]

The National Intelligence Centre is responsible for the security of government networks and classified national security information and manages the government's CERT.[240] Spain has two specialized cyber police forces within the Ministry of the Interior: the National Police Corps' Technological Investigation Brigade and the Civil Guard's Telematic Crime Group.[241] The National Centre for Critical Infrastructure Protection is the body responsible for coordination and critical infrastructure protection,

236 "South African Law on Cybercrime", http://cybercrime.org.za/law.

237 South African Department of Defence, *South African Defence Review 2012*, draft, 2012, p. 214.

238 Spain, *Estrategia Española de Seguridad*, 2011, pp. 13, 38, 43, 69–70, 85.

239 Spanish Ministry of Defence, "Information security", www.defensa.gob.es/en/politica/infraestructura/seguridad-informacion.

240 E. Chamorro and A. Sanz Villalba, "Cybersecurity in Spain: a proposal for its management", Elcano Royal Institute, 29 July 2010; *Spanish National Security Framework*, Royal Decree 3/2010, 8 January 2010, http://administracionelectronica.gob.es/recursos/pae_000002018.pdf.

241 European Network and Information Security Agency, *Spain Country Report*, 2011, p. 26.

including cybersecurity.[242] Spain's CERT was established in 2006.[243] Spain has ratified the Convention on Cybercrime.

Royal Decree 3/2010 adapted the National Security Framework to include prescriptions for cybersecurity practices for the public sector to ensure access, integrity, and confidentiality of information. It stresses that public networks should adopt multilayered "defence in depth" strategies, and that security will include measures of prevention, detection, and mitigation.[244] Although it does not lay out principles for pre-emptive or retaliatory action beyond national borders, preventive measures include not only lessening exposure to potential threats but also dissuasion. The Defence Ministry participates in national, European, and NATO cybersecurity efforts.[245]

Sri Lanka

In February 2011, the Commander of the Sri Lankan Army said that the country faces threats in cyberspace,[246] and that online surveillance and defence against information threats is a priority falling in part on the Ministry of Defence Media Division.[247] The national CERT is the focal point for cyber security, and was established under the Information and Communication Technology Agency; it joined the Asia Pacific CERT in February 2012.[248]

---

242 See Spanish National Centre for Critical Infrastructure Protection, "CNPIC—cibersecurity", www.cnpic-es.es/Ciberseguridad/index.html.

243 Forum of Incident Response and Security Teams, "CCN-CERT", www.first.org/members/teams/ccn-cert.

244 M. Amutio, "National Security Framework of Spain", 13 November 2012, www.epractice.eu/en/cases/ens.

245 E. Chamorro and A. Sanz Villalba, "Cybersecurity in Spain: a proposal for its management", Elcano Royal Institute, 29 July 2010, p. 6.

246 Sri Lankan Ministry of Defence and Urban Development, "'Be prepared for the cyber war after the physical war'—Commander of the Army", 23 February 2011.

247 Sri Lankan Ministry of Defence and Urban Development, "Organisational structure", www.defence.lk/main_abt.asp?fname=orgstr.

248 Sri Lanka CERT, "About us", www.slcert.gov.lk/aboutus.html; Sri Lankan Information and Communication Technology Agency, "Sri Lanka CERT joins APCERT to mitigate cyber threats", 21 February 2012.

Switzerland

The National Strategy for Switzerland's Protection against Cyber Risks, released in June 2012, outlines Switzerland's goals for cyberdefence. The Federal Council is pursuing increased resilience of critical infrastructure, and the reduction of risks, crime, espionage, and sabotage in the cyber domain.[249]

The Federal Department of Defence intends to develop cyber defence, exploitation, and attack capabilities.[250] The Defence Minister stated in 2011 that between 5 and 10 percent of the total defence budget was allocated to cybersecurity.[251] The Centre for Electronic Operations of the Armed Forces Command Support Organization is creating two cyberwar-related units. The first of these is a military CERT, which will be tasked to monitor the systems and networks of the armed forces. It will coordinate with the government CERT.[252] The other is a unit for computer network operations. The Federal Intelligence Service, part of Department of Defence, focuses on the protection of critical information infrastructure.[253]

Turkey

In November 2012, Turkey established the Cyber Security Board, tasked with determining and implementing cybersecurity measures.[254] The Information and Communications Authority and the Scientific and Technological Research Council are working to draft a national

249 Swiss Federal Department of Defence, Civil Protection, and Sport, *National Strategy for Switzerland's Protection against Cyber Risks*, 19 June 2012.

250 Swiss Federal Council, *Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz*, 23 June 2010, p. 32.

251 "Switzerland 'vulnerable to cyber attacks'", *The Local*, 20 July 2011.

252 Swiss Federal Department of Justice and Police, and Federal Department of Foreign Affairs, "Gutachten über Rechtsgrundlagen für Computernetzwerkoperationen durch Dienststellen des VBS", 10 March 2009, www.parlament.ch/d/organe-mitglieder/delegationen/geschaeftspruefungsdelegation/gutachten-zhd-gpdel/Documents/gutachten-ejpd-computernetz-vbs-2009-03-10-d.pdf.

253 Swiss Federal Department of Defence, Civil Protection, and Sport, "The Federal Intelligence Service FIS", www.vbs.admin.ch/internet/vbs/en/home/departement/organisation/ndb.html.

254 "Turkey establishes Cyber Security Board", *Anadolu Agency*, 3 November 2012.

cybersecurity strategy, planned for release in 2013. The Authority will play a supervisory and coordinating role.[255] Turkey announced the establishment of its first civilian cybersecurity organization, the National Cyber Security Coordination Foundation, in October 2011. The Foundation will hire 200 personnel to provided cybersecurity assistance to government institutions and private entities.[256] Turkey merged two agencies in 2010 to create a new entity that is tasked to intercept signals and secure Turkey's electronic communications. It will be staffed by researchers to study cryptography, cybersecurity, electronic warfare, and develop software for the public and private sectors.[257]

Turkey's military strategy, revised in October 2010, added cybersecurity threats.[258] Turkey plans to establish a Cyber Army Command to counter cyberattack against the country, with a special unit within the General Staff to deal with cyber threats, in cooperation with the Defence Ministry, the Scientific and Technological Research Council, and Middle East Technical University.[259] The Command will be subordinated to the General Staff, but have its own budget and an autonomous structure. It will monitor the entire internet in Turkey and offer protection to state institutions.[260]

Ukraine

Ukraine began emphasizing cybersecurity in 2002, when the Ministry of the Interior developed units to counter high-tech crime. Around that time, a department was created at the Ministry's Donetsk Law Institute specifically pertaining to information technologies.[261] Ukraine continues to develop its cybercapabilities and plans. During the 2011 NATO–Ukraine International Staff Talks on Cyber Defense, National Security and Cyber

255 "Turkey's cyber defense plan to be ready in 2013", *Hürriyet Daily News*, 2 March 2012.
256 "Turkey readies itself against cyber attacks", *Today's Zaman*, 2 October 2011.
257 "Turkey creates its own 'NSA'", *TR Defence*, 9 September 2010.
258 "New edition of Turkish Red Book shapes new security spheres", *Hürriyet Daily News*, 28 October 2010.
259 E. Yavuz, "Turkey to mobilize against cyber-terrorism", *Today's Zaman*, 30 January 2011.
260 Ibid.
261 V. Golubev, "Fighting cybercrime in CIS: strategy and tactics", Computer Crime Research Center, 29 June 2005.

Defence Council members briefed attendants on the Draft Strategy of Ukraine on Cyber Defence.[262]

The State Service for Special Communication and Information Protection develops policy on the protection of state information resources and ensures government communications systems function.[263] The Security Service is responsible for protecting the "technical and defence potential of Ukraine".[264] The state's cybersecurity structure continues to develop. In an April 2012 interview, the head of the Security Service noted that Ukraine is creating a Department of Counterintelligence Protection of State Interests in the Field of Information Security in response to numerous attempts to gain unauthorized access to state resources. Additionally, the Security Service proposed creating a national system to fight cybercrime.[265]

The military's role in dealing with cyber threats is outlined in a white paper. It states that "the Armed Forces and other military formations should be capable to participate in ensuring reliability and safety of the national information system".[266] In June 2012, the National Security and Defence Council approved the new Military Doctrine, which states that Ukraine considers cyberattacks on nuclear facilities, the chemical and defence industries, military stores, and economic and information entities as grounds for armed conflict.[267] While its military capabilities remain uncertain, the General Staff includes a Central Directorate for Information Security and Cryptology.[268] Ukraine has ratified the Convention on Cybercrime.

---

262 Ukrainian Security Service, "NATO–Ukraine International Staff Talks on Cyber Defense in Yalta", 20 October 2011.

263 Ukrainian State Service for Special Communication and Information Protection, "Tasks", 3 December 2010, www.dstszi.gov.ua/dstszi/control/en/publish/article?art_id=89931&cat_id=89930.

264 Ukrainian Security Service, "Objectives and duties of the SSU", www.sbu.gov.ua/sbu/control/en/publish/article?art_id=83745&cat_id=83637.

265 Ukrainian Security Service, "The SSU Head: averting terrorist threats in the course of preparation and holding of Euro-2012 in Ukraine is one of the main tasks of the special service", 10 April 2012.

266 Ukrainian Ministry of Defence, *Ukraine's Strategic Defence Bulletin until 2015 (Defence White Paper)*, 2004, p. 16.

267 See www.rnbo.gov.ua/documents/304.html.

268 Ukrainian Ministry of Defence, *White Book 2011: Armed Forces of Ukraine*, 2012, p. 75.

United Kingdom

The United Kingdom has one of the most advanced national approaches to cybersecurity. In November 2011, the United Kingdom updated its Cyber Security Strategy. The Strategy characterizes cyberattack as a national security threat. The Strategy's objectives include addressing cybercrime and creating a secure business environment, enhancing information infrastructure resiliency, ensuring an open, safe cyberspace for the public, and developing an adequate cybersecurity workforce. The Strategy says the United Kingdom will work bilaterally and through international forums to establish international norms and develop confidence-building measures.[269]

The government has allocated £650 million through 2015 to implement the National Cyber Security Programme. Two thirds of this funding will be allocated to developing "operational capabilities", and 20 per cent to public and private critical cyber infrastructure. Almost half will be allocated to the Government Communications Headquarters, the national signals intelligence agency.[270] The Office of Cyber Security and Information Assurance, created in 2009, provides strategic direction and coordinates cybersecurity policy from within the Cabinet Office.[271] It is responsible for implementing the National Cyber Security Programme and managing the £650 million budget.[272] The Centre for the Protection of National Infrastructure provides guidance to critical infrastructure owners on cyber threats and operates information exchanges to facilitate public–private information-sharing on threats and protective measures.[273]

---

269 United Kingdom, *The UK Cybersecurity Strategy: Protecting and Promoting the UK in a Digital World*, 2011, pp. 5, 8, 26–27.

270 "Defence Cyber Operations Group", presentation by the Cyber and Influence Science and Technology Centre, 1 November 2011, www.science.mod.uk/controls/getpdf.pdf?606.

271 UK Cabinet Office, "Office of Cybersecurity and Information Assurance (OCSIA)", https://update.cabinetoffice.gov.uk/content/office-cyber-security-and-information-assurance-ocsia.

272 "Defence Cyber Operations Group", presentation by the Cyber and Influence Science and Technology Centre, 1 November 2011, www.science.mod.uk/controls/getpdf.pdf?606.

273 UK Parliamentary Office of Science and Technology, "Cyber security in the UK", *Postnote*, no. 389, September 2011.

In September 2012, the United Kingdom announced the creation of an academic institute dedicated to researching cybersecurity. It is backed by the Government Communications Headquarters and will increase resiliency against cyberattack and better equip the government to defend the country's interests in cyberspace.[274] The United Kingdom will also establish a National Crime Agency, to include a national cybercrime unit to investigate and respond to serious national-level cybercrime and provide support and training to local police forces. This unit will be created by combining the Serious Organized Crime Agency and the Metropolitan Police's e-crime units.[275] In March 2012, the Revenue and Customs Service announced that it would establish a cybercrime team to investigate cyber-abetted tax fraud.[276]

The 2010 National Security Strategy highlights "hostile attacks upon UK cyber space by other states and large scale cybercrime" as among the highest priorities. The updated 2011 Strategy states that the new Joint Forces Command will lead development and integration of cyber defence capabilities. The Strategy also calls for the creation of two Joint Cyber Units. One will be within the Global Operations and Security Control Centre to "proactively and reactively" defend Ministry of Defence networks against attack. The second unit will be within Government Communications Headquarters, with responsibility to develop "new tactics, techniques, and plans to deliver military effects … through operations in cyberspace".[277]

The 2009 Cyber Security Strategy called for the Ministry of Defence to create a Cyber Security Operations Center, located in the Government Communications Headquarters, responsible for developing both offensive and defensive cybercapabilities.[278] The 2010 Strategic Defence and Security Review called for the creation of a Defence Cyber Operations

274 D. Meyer, "Spies and professors band together for UK cybersecurity research institute", *ZDNet*, 13 September 2012.

275 United Kingdom, *The UK Cybersecurity Strategy: Protecting and Promoting the UK in a Digital World*, 2011, p. 30.

276 D. du Preez, "HMRC sets up new cyber-crime team to tackle tax fraud", *CIO*, 13 March 2012.

277 UK Parliament, "HC 106 Defence and Cyber-security: supplementary written evidence from the Ministry of Defence following the private evidence session on 18 April 2012", www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/writev/106/m01a.htm.

278 United Kingdom, *Cybersecurity Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space*, 2009, p. 17.

Group. The Group, to be operational by March 2015, will be a "federation of cyber units across defence", to "ensure the coherent integration of cyber activities across the spectrum of defence operations".[279] Within the Ministry of Defence, the Global Operations and Security Control Centre is responsible for defending the Ministry's network.

United States

The United States is undertaking an extensive cybersecurity programme, both in the civilian and military realm, with a number of significant actions in 2012. The United States completed a Cyberspace Policy Review in May 2009, and in December 2009 appointed a mid-level Cybersecurity Coordinator to the staff of the National Security Council.[280] Many of the provisions in the Cyberspace Policy Review are also found in the 2010 National Security Strategy.[281] Responsibility for cybersecurity is divided among the Department of Homeland Security, the Federal Bureau of Investigation, and the Department of Defence, including US Cyber Command (which has the National Security Agency as one of its components), with the Departments of State and Commerce leading international negotiations and the development of cybersecurity standards

The Department of Homeland Security's National Cybersecurity Division is tasked to "work collaboratively with public, private, and international entities to secure cyberspace and America's cyber interest".[282] The Division has a number of programmes to assist companies in protecting cyber infrastructure from attack.[283] The National Cyber Response Coordination Group is comprised of 13 federal agencies and is responsible for coordinating the federal response in the event of a "nationally significant cyber incident".[284] The Department of Homeland Security also has

279 United Kingdom, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, 2010, p. 27.

280 The White House, "Cybersecurity", www.whitehouse.gov/administration/eop/nsc/cybersecurity.

281 United States, *National Security Strategy*, 2010.

282 US Department of Homeland Security, "National Cyber Security Division", www.dhs.gov/xabout/structure/editorial_0839.shtm.

283 See US Department of Homeland Security, "Homeland Security Presidential Directive 7: critical infrastructure identification, prioritization, and protection", 17 December 2003.

284 US Department of Homeland Security, "National Cyber Security Division", www.dhs.gov/xabout/structure/editorial_0839.shtm.

expanded the work of the National Cybersecurity and Communications Integration Center to improve situational awareness and information-sharing. The Department of Defence and the Department of Homeland Security signed a memorandum of agreement in October 2010 to increase interdepartmental collaboration.[285]

In 2012, the Congress twice failed to pass administration-backed legislation that would have given the Department of Homeland Security the authority to secure critical infrastructure networks.[286] The failure of legislation prompted an announcement by the White House that the President would issue an executive order (which has the force of law) establishing some minimal requirements for improving security at critical infrastructures.

It has been reported that, in October 2012, President Obama signed a Presidential Decision Directive governing military activities in cyberspace. The Directive itself is classified but remarks by the Secretary of Defense suggest that the military will play a greater role in defending against cyberattack from foreign sources.[287] Secretary of Defense Leon Panetta, in a speech on 18 December 2012, said that the Department of Defense had recently developed new rules of engagement in cyberspace that clarified its mission to defend the country, and that will enable it "to more quickly respond to cyber threats".[288] He further stated that the Department of Defense is exploring ways to strengthen the Cyber Command, currently a sub-command of the Strategic Command. The Cyber Command, established in 2010 and originally responsible for dealing with threats to the military cyber infrastructure, will now have broader national cyberdefence responsibilities because of the Presidential Directive. The Command is responsible for both defensive and offensive operations.[289] Cyber Command's service elements include Army Forces Cyber Command, the

285 Memorandum of Agreement Between the Department of Homeland Security and the Department of Defence Regarding Cybersecurity, 13 October 2010, www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

286 M. Clayton, "Senate cybersecurity bill fails, so Obama could take charge", *Christian Science Monitor*, 16 November 2012.

287 E. Nakashima, "Obama signs secret directive to thwart cyberattacks", *Washington Post*, 14 November 2012.

288 "The force of the 21st century", as delivered to the National Press Club by US Secretary of Defense Leon E. Panetta, Washington, DC, 18 December 2012, www.defense.gov/speeches/speech.aspx?speechid=1742.

289 Z. Fryer-Briggs, "U.S. military goes on cyber offensive", *Defense News*, 24 March 2012.

Twenty-fourth Air Force, Fleet Cyber Command and Marine Forces Cyber Command.[290]

In November 2012, the Defense Advanced Research Projects Agency released a document soliciting research into the conduct of cyberwar, called Foundational Cyberwarfare (Plan X). The document states that, "Plan X will conduct novel research into the nature of cyberwarfare and support development of fundamental strategies needed to dominate the cyber battlespace. Proposed research should investigate innovative approaches that enable revolutionary advances in science, devices, or systems".[291]

Widespread media reports attributed to US national security officials claim that the 2010 "Stuxnet" cyberattack against an Iranian nuclear facility was propagated by the United States and Israel.[292]

Viet Nam

Viet Nam's Ministry of Public Security has proposed the establishment of a high command to provide electronic and cybersecurity for the military, citing the "eventuality of cyber wars" as a key impetus for a cyber-military organization. The Director of the Department of Information Technology within the Ministry of Public Security has been an advocate for improving operational cybercapabilities.[293] The General Department of Logistics and Technology of the Ministry of Public Security, the national CERT, and the International Data Group continue to draft plans for information security advancements throughout the next decade.[294] Viet Nam is planning to invest $42 million to secure sensitive information and to establish a National Centre for Technology and an Agency for Information Security.[295]

---

290 US Department of Defence, "U.S. Cyber Command fact sheet", 25 May 2010, www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf.

291 "DARPA-BAA-13-02, Foundational Cyberwarfare (Plan X)", 21 November 2012, www.fbo.gov/index?s=opportunity&mode=form&id=1bc45a18e1ba0763640824679d331e46&tab=core&_cview=0.

292 D.E. Sanger, "Obama order sped up wave of cyberattacks against Iran", *New York Times*, 1 June 2012.

293 "High command proposed for Vietnam cyber security operations", *Thanh Nien News*, 8 July 2011.

294 "Press release Security World 2011", Citek Corporation, 3 March 2011, www.citek.com.vn/newsdetail.php?id=380&cat_id=1037.

295 "Vietnam boosts its cyber-threat protection", *UPI*, 28 January 2010.

As part of this investment, Viet Nam approved a national master plan to secure domestic cyberspace for the period of 2010–2020 and created the National Network Security Technical Centre to develop a system for monitoring, early warning, and incident response, to be operational within two years.[296] The national CERT, a unit within the Ministry of Information and Communication, was established in 2005. Its tasks include the coordination of cyberincident response and the development of computer network security.[297]

STATES WITH CIVILIAN POLICIES AND ORGANIZATIONS FOR CYBERSECURITY

Afghanistan

The Afghanistan Ministry of Telecommunication and Information Technology is developing a National Cybersecurity Strategy.[298] The first draft of the Strategy is expected to be completed by the end of 2012 and be presented to the information and communication technology council.[299] In May of 2012, NATO and Georgia developed a cyberdefence training programme to educate Afghan network and system administrators to build institutional capability and increase public awareness of cyber threats.[300]

Antigua and Barbuda

Antigua and Barbuda is working with the OAS to establish a national CSIRT. It will function as a point of contact for domestic and regional cyberincident reporting, investigation, response, and information-

296 See Viet Nam's APEC Counter Terrorism Action Plan, p. 1, available at Asia-Pacific Economic Cooperation, "Counter Terrorism Action Plans", www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Task-Groups/Counter-Terrorism-Task-Force/Counter-Terrorism-Action-Plans.aspx.

297 Vietnam Computer Emergency Response Team, "About us", www.vncert.gov.vn/en.

298 "Afghanistan's first ever 'National Policy on Cyber Security'", *Wadsam*, 2 September 2012.

299 Afghan Ministry of Communication and Information Technology, "National conference holds for Afghanistan's cyber security", 2 September 2012.

300 NATO, "Afghan managers train in cyber defence", 21 May 2012.

sharing.[301] As part of this effort, Antigua and Barbuda held the First National Workshop on Cyber Security and Incident Response in 2009 and a 2012 workshop to educate government employees about cyber threats. Antigua and Barbuda is home to the Regional Cyber Forensics Lab, which assists in regional cyber law enforcement, and has started training police officers in cybercrime investigation.[302]

Armenia

In 2009, Armenia created an "intergovernmental target group" to develop the National Concept on Information Security. The Ministry of Transport and Communications, the Ministry of Economy, and the Public Services Regulatory Commission are the three main government agencies in charge of cybersecurity. The Republic of Armenia Government Program of 2008–2012 cites "improving cyber security significantly" as a primary task of national security and law enforcement authorities.[303] The National Research and Education Network Cyberspace Security Strategy of 2006 led to the establishment of a national CSIRT and CERT.[304] To improve its cyberdefence capabilities, Armenia has been working with NATO to develop cyber policies and capabilities and is expected to establish a State Cyber Security Committee.[305]

Azerbaijan

To address cybersecurity challenges, the Azerbaijani Ministry of National Security held a major conference in March 2012 with representatives from Azerbaijan and several European Union member states to discuss information security initiatives, policies to secure e-government, and strategies for minimizing incidents against national infrastructure.[306]

---

301 Antigua and Barbuda, "Ministry holds cyber security awareness workshop for employees", 5 January 2012.

302 Remarks by Lt. Col. Edward H. Croft at the First National Workshop on Cyber Security and Incident Response, 12–15 July 2010, www.antigua.gov.ag/pdf/speeches/remarks_by_edwardH_croft.pdf.

303 Armenia, *Republic of Armenia Government Program*, 2008, p. 54.

304 CERT AM, "About", www.cert.am/node/7.

305 NATO, *Individual Partnership Action Plan 2011–2013: Armenia*, www.mfa.am/u_files/file/IPAP-2011-2013-ENG-Declassified.pdf.

306 "Azerbaijan seeks to improve information security", *Today.Az*, 14 March 2012.

Azerbaijan has joined the Convention on Cybercrime and has established a CERT.[307]

Bangladesh

In 2012, the Bangladesh Telecommunication Regulatory Commission established a CSIRT. Its goals are to detect, prevent, and respond to cyberincidents.[308] It will have a special focus on cybercrime.[309]

Belgium

Responsibility in the Belgian government for cyber defence is spread across various agencies. Belgium does not have a national cybersecurity strategy. The Belgian Network Information Security platform advises the government on cyber threats and critical infrastructure protection. In 2011, the creation of a cybercrime centre was announced.[310] The Modernization Plan 2000–2015 of the armed forces cites "increased computerised actions" as one of the four reasons for the creation of a unified joint staff.[311] Belgium has signed a memorandum of understanding with the Netherlands and Luxembourg for cooperation in cybersecurity, including information- and expertise-sharing as well as cooperation on best practices and the development of public–private partnerships.[312]

Bhutan

The Bhutan government is expected to submit the Bhutan Information Communications and Media Amendment Bill to parliament in 2013. The bill seeks to address all regulatory aspects of the information and communication technology and media sectors, including issues as varied as

307 H. Veliyev, "Deputy Minister: Azerbaijan's information security—part of national security", *Trend*, 4 May 2011.
308 Bangladesh CSIRT, "About us", http://csirt.gov.bd/?q=node/1.
309 "BTRC moves against cybercrimes", *bdnews24.com*, 25 January 2012.
310 European Network and Information Security Agency, *Belgium Country Report*, 2011, p. 5.
311 J. Ondřejka and R. Stojar, "Belgian Armed Forces: trends in development", *Defence and Strategy*, no. 2, 2003, p. 112.
312 European Urban Knowledge Network, "Benelux sign memorandum of understanding on cyber security", 12 April 2011.

child pornography, identity fraud, and cyberterrorism.[313] It will also address cybersecurity functions with the establishment of a national CSIRT.[314] The proposed CSIRT will coordinate cyberincident response, as well as advise on cybersecurity procedures, prevention, and response.[315]

Brunei Darussalam

The CERT of Brunei Darussalam was formed in May 2004 in collaboration with the Ministry of Communication.[316] It has 44 employees and coordinates with other national CERTs, businesses, government agencies and internet service providers. In November 2011, Brunei Darussalam hosted the first Interactive Technical Workshop on cybersecurity incident response for the Organization of Islamic Cooperation CERT.[317] The government focuses on employing cybercapabilities defensively, protecting internal systems, and promoting information technology development.[318]

Bulgaria

In October 2011, Bulgaria announced its intent to establish a National Cyber Security Authority that would set up a regulatory framework to coordinate the country's cybersecurity efforts and strengthen the role of the national CSIRT.[319] The Authority will be comprised of reserve officers and specialists from the information technology community to share information and offer cyber training and education programmes.[320]

---

313 "Bhutan Information Communications and Media (BICM) Amendment Bill", *Bhutanomics: The Bhutan Analytics*, 26 September 2012.

314 M. Dorji, "Final BICMA Act draft goes to Cabinet", *The Bhutanese*, 31 March 2012.

315 "Bhutan Computer Incidence Response Team", *Bhutanomics: The Bhutan Analytics*, 22 September 2012.

316 CERT of Brunei Darussalam, "About BruCert", www.brucert.org.bn.

317 H. Hayat, "Brunei privileged to host first ever workshop on cyber security incident response, handling", *BruDirect.com*, 22 November 2011.

318 *Brunei Darussalam Public Sector Journey towards E-Government*, paper from 12th ASEAN Conference on Civil Service Matters, 13–15 October 2003, www.bruneiresources.com/pdf/accsm12_brunei_countrypaper.pdf.

319 "Bulgaria to establish National Cyber Security Authority", *Xinhua*, 19 October 2011, http://news.xinhuanet.com/english2010/world/2011-10/19/c_131201077.htm.

320 Address by the Deputy Minister of Defence Valentin Radev, Sofia, 28 September 2010, www.atlantic-bg.org/images/news/round-table-cyber-sec-28_09-2010/

In addition, a Ministry of Defence white paper states that Bulgaria is focused on consolidating its information networks "so as to build a single information network". This interconnectedness will require "vigilance on the part of military formations for its maintenance and security".[321]

Burundi

Burundi intends to set up a national CERT with assistance from the International Telecommunication Union.[322] The government emphasizes the importance of a "strong culture of cybersecurity" based on the East African Community Framework for Cyberlaw, which requires all Community members to pass cybersecurity legislation consistent with the principles of the Convention on Cybercrime.[323] As of May 2012, Burundi and Rwanda are working to strengthen bilateral law enforcement ties to enable their national police forces to collaborate on cross-border crime, citing cybercrime as a major threat.[324] Burundi is also building its capacity to participate in a global cybercrime investigation network.[325]

Cambodia

The Cambodian government is currently drafting its first cyber law.[326] In 2007, Cambodia formed a national CERT. Its tasks include responding to computer security incidents within the country, the development of a Cyber Security Platform, and a cybercrime law initiative. It is composed of a "non-profit team of IT security professionals".[327]

---

docs/radev-privetstvie-28-09-10.pdf.

321 Bulgarian Ministry of Defence, *White Paper on Defence and the Armed Forces of the Republic of Bulgaria*, 2010.

322 US Department of State, "Declaration of delegates from Kenya, Tanzania, Uganda, Rwanda and Burundi from the 2011 East African Workshop on Cyberspace Security", 27 July 2011.

323 B.R. Asiimwe, "EAC joins fight against cyber crimes", *New Times*, 4 August 2011.

324 F. Ndoli, "Rwanda: country partners with Burundi to fight crime", *All Africa*, 8 May 2012.

325 "East Africa: Board joins fight against cyber crimes", *All Africa*, 4 August 2011.

326 Cambodian Center for Human Rights, "Cambodian Government is drafting the first ever Cyber Law", 24 May 2012.

327 Cambodia CERT, "Who we are", www.camcert.gov.kh/?page_id=664.

Cameroon

In 2012, Cameroon launched the Public Key Infrastructure centre in an effort to make online information more secure.[328] The government introduced a law on cybercrime in December 2010 that defines different types of cybercrime and sets the foundation for a cyber police force to be established.[329]

Cyprus

In 2004, Cyprus passed a cybercrime law covering illegal access, data interception or interference, misuse of devices, and cyber forgery and fraud. The law also ratified the Convention on Cybercrime. CyberEthics, a partnership of government agencies, the media, and internet service provider associations, allows police to work with private companies in investigating cybercrime incidents.[330] In addition, the Cyprus Police Force has a unit that focuses on cybercrime investigations and has collaborated with the Ministry of Education and Ministry of the Interior to educate people on safe internet use and cybercrime prevention. Two national CERTS (one for government, and one for academia and the private sector) were established in 2010.[331]

Czech Republic

The Cyber Security Strategy of the Czech Republic for 2011–2015 lays the groundwork for future security policies and legal standards. The underlying objective of the strategy is to protect ICT infrastructure from cyber threats and to mitigate the consequences of attacks if they occur.[332] In October 2011, the Czech Republic released Decision 781, establishing

328 T. Nanyongo, "Public key infrastructure launched in Yaounde", Cameroon Radio Television, 2 November 2012; see also "Cameroon, ICT hub of Central Africa", *oAfrica*, 18 December 2012.

329 S. Tembang Mforgham, "Cameroon to set up cyber police force", *Africa News*, 30 June 2010.

330 European Network and Information Security Agency, *Cyprus Country Report*, 2011, pp. 7–8, 12.

331 Ibid., p. 24.

332 *Cybersecurity Strategy of the Czech Republic for the 2011–2015 Period*, www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.pdf.

the National Security Authority, charged with cybersecurity. Decision 781 also established the National Centre for Cybernetic Security, which coordinates with Czech and international CERTs and undertakes research and development.[333] The Czech Republic also signed a memorandum of understanding on cybersecurity cooperation with NATO in March of 2012.[334]

The strategy considers cybersecurity the responsibility of the government, private sector, and general population, and as a result the government will draft legislation to determine the responsibilities of the relevant public authorities for establishing cybersecurity standards for the government, private sector, and individual computer users. The Czech Republic plans to pass legislation to establish security standards for critical infrastructure, and to create a national CERT that will provide cyber threat early warning and optimize response capabilities.[335] The Ministry of Interior coordinates cybersecurity issues.[336] The National Security Research Strategy, approved in 2008, includes protection of critical infrastructure, and is implemented by the Ministry of the Interior, which has a Cyber and Informational Security Department.[337]

Dominican Republic

The President's Office of Information Technology and Communication states that it is responsible for information security. The Dominican government has also established an Inter-Institutional Commission against High-Technology Crimes, which brings together various government departments to coordinate cybersecurity efforts and make policy recommendations.[338] The Commission includes the armed forces, national

333 Czech National Cybersecurity Center, "What is NCK", www.govcert.cz/en.

334 Permanent Delegation of the Czech Republic to NATO in Brussels, "Czech Republic signed a MoU on cybersecurity cooperation with NATO", 19 March 2012.

335 *Cybersecurity Strategy of the Czech Republic for the 2011–2015 Period*, www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.pdf.

336 "Cybersecurity in the Czech Republic", *CyberSecurity.cz*, ww.cybersecurity.cz/basic_en.html.

337 European Network and Information Security Agency, *Czech Republic Country Report*, 2011, pp. 5, 13.

338 Dominican Presidential Office of Information Technologies and Communications, "¿Qué es la OPTIC?", www.optic.gob.do/SobreNosotros/

police, the Dominican Institute of Telecommunications (Indotel), the Directorate for Counternarcotics, the Ministry of Interior and Police, National Department of Investigations, the Superintendency of Banking, the Technology Institute of Latin America, and the child-protection agency Conani.[339] The National Police's Investigatory Department of High-Technology Crimes, the national cyber-crime unit, investigates threats and attacks on national critical infrastructure.[340] The Armed Forces J-2 Intelligence Directorate provides information and support to these investigations. In 2007, the National Congress approved Law 53-07 against High-Tech Crimes, which defines computer-related crimes.[341]

Egypt

Egypt's Ministry of Communications and Information Technology developed in 2007 the CyberSecurity Initiative (2007–2009) to improve safety and the security. This followed on earlier actions to make cybersecurity part of the responsibilities of the National Security Council and the establishment of a cybersecurity committee in the Ministry. The Information Technology Industry Development Agency, which is part of the Ministry, is responsible for improving cybersecurity and data protection. In April 2010, Egypt established a CERT as part of the National Telecom Regulatory Authority.[342] The CERT provides incident response, defence, and analysis against cyberattacks and collaborates with other agencies on to deal with online threats and emergencies.[343]

Qui%C3%A9nesSomos/tabid/61/Default.aspx.

339 G. Diniz and R. Muggah, *A Fine Balance: Mapping Cyber (In)Security in Latin America*, Instituto Igarapé, 2012, p. 16.

340 Dominican Republic National Police, "Departamento Investigacion de Crimenes de Alta Tecnologia, P.N.(DICRIM)", www.policianacional.gob.do/v2/dicrim/departamentos/20110224-dicat.ashx.

341 G. Diniz and R. Muggah, *A Fine Balance: Mapping Cyber (In)Security in Latin America*, Instituto Igarapé, 2012, p. 12.

342 Egyptian Computer Emergency Response Team, "About EG-CERT", www.egcert.eg/cert/about.html.

343 Arab Republic of Egypt Ministry of Communications and Information Technology, "The Egyptian Computer Emergency Response Team (CERT): press kit", 18 August 2009, http://mcit.gov.eg/Media_Center/Press_Room/Press_Kits/813.

Ethiopia

In 2010, the Ethiopian government updated its criminal code in order to ensure that cybercrimes were specifically defined and that hackers could face criminal charges. This law was enacted primarily to protect financial institutions, which were attempting to confront the cyber threat but were not adequately protected by law.[344] The Ethiopian ICT Development Authority has an action plan that includes a goal of "addressing national security and law and order issues to support and promote ICTs exploitation in the country".[345]

Ghana

Ghana's intention of becoming the information hub of West Africa has led the government to enact cybercrime legislation and enhance cybersecurity practices.[346] Acting on that goal, in 2008 Ghana passed the Electronic Communications Act and the Electronic Transactions Act, which established the legal framework for governing information technology.[347] In November 2011, the Deputy Minister for Communications announced the development of a national cybersecurity strategy, aimed at combating cybercrime and securing critical infrastructure.[348] In June 2012, the National Information Technology Agency announced a national CERT "strategy" designed to coordinate government response to cyberattacks, both internal and external. The Agency also aims to establish CERTs

344 "Ethiopia to adopt 'cyberlaw'", Kulfo Research and Development, 19 July 2010, http://kulfo.wordpress.com/2010/07/19/ethiopia-to-adopt-%E2%80%98cyberlaw%E2%80%99.

345 J. Suhonen, "Ethiopian Information and Communication Technology Development Agency (EICTDA)", 22 September 2011, http://wiki.uef.fi/display/IMPDET/Ethiopian+Information+and+Communication+Technology+Development+Agency+%28EICTDA%29.

346 J. Coomson, "Ghana: cyber crimes in Ghana", *Ghanian Chronicle*, 4 October 2006.

347 Parliament of the Republic of Ghana, *Electronic Transactions Act, 2008*, 19 December 2008, www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/WPFD2009/pdf/Ghana%20Electronic-Communications%20Act%202008.pdf.

348 E. Awuah, "Ghana's data vulnerable", *Daily Guide Ghana*, 29 November 2011.

for each municipal, metropolitan, and district assembly to improve coordination and information-sharing on cyber threats.[349]

Grenada

In August 2012, Grenada announced the establishment of a national computer incident response team (CIRT). The CIRT was indicated as an important part of new approaches to deal with cybersecurity, cyberterrorism, and other cyber threats.[350] The CIRT will coordinate action at both the national and regional levels to identify threats and be the country's focal point for cybersecurity matters.[351]

Iceland

Currently, cybersecurity responsibilities are divided among the Ministry of the Interior, the Post and Telecom Administration, and the National Commission of the Icelandic Police. The Ministry of the Interior is developing a national strategy. A national CERT is in the process of being created and reportedly the team should be operational in 2012.[352] Iceland ratified the Convention on Cybercrime in 2007.

Ireland

Ireland is drafting a Criminal Justice (Cybercrime) Bill, which would define crimes related to information systems and data. It would allow ratification of the Convention on Cybercrime and adoption of the European Union Framework Decision on attacks against information systems.[353] The Department of Justice and Equality Strategy Statement 2011–2014 indicates that future action will include "continu[ing] to develop policy in

349 "NITACERT to limit cyber attack on govt information", *Ghana News Agency*, 24 June 2012.

350 Government of Grenada, "Grenada taking steps to improve cyber-security", 22 August 2012, www.gov.gd/egov/news/2012/aug12/22_08_12/item_2/grenada_taking_steps_improve_cyber_security.html.

351 "Grenada looks to boost cybersecurity", *Caribbean Journal*, 23 August 2012.

352 European Network and Information Security Agency, *Iceland Country Report*, 2011.

353 "UCD to lead EU initiative for training cyber cops", *Silicon Republic*, 1 June 2011.

relation to combating organized crime and cybercrime".[354] The National Police have a Cybercrime Investigation Unit responsible for investigating computer-related crime.[355] The Irish Reporting and Information Security Service CERT is the main cybersecurity resource for the government and businesses.[356]

Jamaica

Jamaica's National Security Policy called cybercrime one of the key criminal threats to national security. It has assigned the Ministry of Industry, Technology, Energy and Commerce responsibility for developing a robust, secure network to support critical financial infrastructure as a key capability towards providing a stable economy and effective social services delivery.[357] In 2010, the Cybercrimes Act entered into force, criminalizing hacking, the dissemination of worms and viruses, unauthorized access, information interception, and obstruction of computer operations.[358] Furthermore, in 2010 the Jamaica Constabulary Force created a Communication Forensics and Cyber Unit within its Organized Crime Investigation Division, and assigned this unit responsibility for investigating crimes using any form of digital media.[359]

Jordan

Jordan's Ministry of Information and Communications Technology is developing a draft national strategy for information security. The National Information Assurance and Cyber Security Strategy calls for the creation

354 Ireland Department of Justice and Equality, *Strategy Statement 2011–2014*, www.justice.ie/en/JELR/Strategy%20Statement%20_English_%202011-2014.pdf/Files/Strategy%20Statement%20_English_%202011-2014.pdf/.

355 Ireland National Police Service, "Garda Bureau of Fraud Investigation", www.garda.ie/Controller.aspx?Page=29.

356 Irish Reporting and Information Security Service, "Welcome", www.iriss.ie/iriss/index.htm.

357 Government of Jamaica, *National Security Policy for Jamaica: Towards a Secure and Prosperous Nation*, 2006, pp. 15, 76.

358 Jamaican House of Parliament, *The Cybercrimes Act, 2010*, 16 March 2010, www.japarliament.gov.jm/attachments/341_The%20Cybercrimes%20Act,%202010.pdf.

359 Jamaica Communication Forensics and Cybercrime Unit, *Project Proposal for CFCU 2012*, p. 1.

of a national CERT and a national critical infrastructure protection programme, as well as the establishment of a National Information Assurance and Cybersecurity Agency.[360] In 2010, the Jordanian Cabinet approved the Information System Crimes Law, issued by the Ministry of Information and Communication Technology.[361] The National Centre for the Security and Assurance of Information and Communication Systems of the Hashemite University has three laboratories to train students on combating cybercrime.[362]

Kenya

Kenya's Communications Commission operates a CIRT, responsible for national cybersecurity incident coordination and management.[363] In February 2012, the government signed an agreement with the International Telecommunication Union to fund the creation of a Kenyan National Computer Incident Response Team Coordination Centre.[364] As well, the government participates in regional cybersecurity workshops that address the rule of law and freedom of expression in cyberspace.[365] Kenya is involved with the East African Community, which has expressed interest in developing cyber law to underpin the Common Market Protocol.[366] In 2011, the United States Trade and Development Agency awarded a US$ 580,000 grant to Kenya's Ministry of Information and Communications to develop a National Cybersecurity Master Plan, which will outline minimum

360 International Telecommunication Union, *ICT Adoption and Prospects in the Arab Region*, 2012, p. 61, www.itu.int/dms_pub/itu-d/opb/ind/D-IND-AR-2012-PDF-E.pdf.

361 R. Olwan, "New cyber crime law in Jordan", *olwan.org*, 13 August 2010.

362 M. Ghazal, "Local cybercrime centre to serve region", *Jordan Times*, 16 February 2011.

363 Communications Commission of Kenya, "Functions of the KE-CIRT/CC", www.cck.go.ke/industry/information_security/ke-cirt-cc/functions.html.

364 "Kenya signs MoU to boost cyber-security", *Daily Nation*, 27 February 2012.

365 C. Painter, "East Africa workshop to address cyber security", *DipNote*, 22 July 2011, http://blogs.state.gov/index.php/site/entry/east_africa_workshop_cyber_security.

366 East African Community Secretariat, "EAC develops cyber laws", 26 October 2011, www.eac.int/infrastructure/index.php?option=com_content&view=article&id=144:eac-develops-cyber-laws&catid=40:press&Itemid=149.

cybersecurity standards and develop a security framework for national information networks.[367]

Kuwait

Kuwait's Central Agency for Information Technology is responsible for cybersecurity, and is considering the development of a National Information Security Framework and a CERT for Kuwait.[368] Kuwait created an anti-cybercrime directorate under the Ministry of Interior's Directorate General for Criminal Investigations in 2008. In 2012, the United Kingdom and Kuwait agreed on a security assistance package that includes cybersecurity.[369]

Latvia

Latvia's 2012 National Security Concept and State Defence Concept prioritize the protection of critical communications infrastructure, highlight the threat of cyberattack, and emphasize ensuring information superiority to ensure flexibility in responding to cyberattack.[370] The Information Technology Security Act, which came into effect in 2011, requires every state department in Latvia to appoint a Head of Security for information technology to ensure that data is kept safe in case of emergency or natural disaster. The Act also requires creation of a Cyber Security Response Agency, which will merge two existing computer security institutions and

---

367 United States Trade and Development Agency, "USTDA supports Kenya's efforts to secure its growing telecommunications infrastructure", 23 September 2011, www.ustda.gov/news/pressreleases/2011/SubSaharanAfrica/Kenya/KenyaNationalCyberscurity_092311.asp.

368 See Arabian Conference on Information and Communications Security, "Recommendations the Second Arabian Conference on Information and Communications Security September 24–25, 2012", www.acics.com.kw/final%20re.html.

369 "UK and Kuwait to announce security partnership", *BBC*, 28 November 2012.

370 Latvian Ministry of Defence, *The State Defence Concept: Executive Summary*, 2012, pp. 6–7, 9, www.mod.gov.lv/lv/Par_aizsardzibas_nozari/Politikas_planosana/Koncepcijas/~/media/AM/Par_aizsardzibas_nozari/Plani,%20koncepcijas/2012_va_EN.ashx; Latvian Ministry of Foreign Affairs, "The National Security Concept", 24 January 2012, www.mfa.gov.lv/en/security/basic/4534/#_Toc10954567.

will consist of eight experts who will oversee compliance with the act. Currently, the Ministry of Transport is responsible for information security policy development. Future government CERT/CSIRT programmes will include monitoring, risk assessment, recommendations, incident handling and assistance, awareness raising, exercises, and research.[371]

Lebanon

In September 2012, Lebanon's Justice Minister announced the finalization of a draft law that would organize the country's electronic sectors and bolster efforts to counteract cybercrime.[372] In 2009, Lebanon launched the Cybercrime and Intellectual Property Bureau as part of its Internal Security Force. Lebanon enacted a data-protection law covering manipulation of personal data. Efforts have been made to join the Convention on Cybercrime, however, as of yet, Lebanon does not participate in the treaty.[373]

Liechtenstein

Liechtenstein signed the Convention on Cybercrime in 2008, and in 2009 amended its penal code to levy penalties for unauthorized computer access, data interception, disruption of a computer system, and data corruption. Child pornography is also prohibited.[374] Under an agreement with Liechtenstein's National Police, Switzerland's Cybercrime Coordination Unit investigates reports of cybercrime in Liechtenstein. Similarly, Switzerland's CERT provides services to Liechtenstein as well.[375] Domestically, the Office of Communications is the national regulatory authority with responsibility for monitoring electronic communications.

---

371 European Network and Information Security Agency, *Latvia Country Report*, 2011, p. 9.

372 "Lebanon to bolster measures against electronic crimes", *The Daily Star*, 25 September 2012.

373 United Nations Economic and Social Commission for Western Asia, *National Profile of the Information Society in Lebanon*, UN document E/ESCWA/ICTD/2011/4/Add.1, 15 November 2011.

374 Family Online Safety Institute Global Resources Information Directory, "Liechtenstein", 9 August 2011, www.fosigrid.org/europe/liechtenstein.

375 L. Jorio, "Cleaning up Switzerland's internet sites", *swissinfo.ch*, 4 September 2012.

Luxembourg

Luxembourg's national cyber strategy was launched in 2003 by the Ministry of the Economy and Foreign Trade. Its primary objectives were to enhance public awareness, incident prevention measures, recovery capabilities, and investigation and forensics.[376] In 2011, Luxembourg released an updated cybersecurity strategy that highlights five key elements: protecting critical infrastructure, modernizing the legal framework for cybersecurity, engaging in national and international cooperation, educating the public and raising awareness, and establishing binding norms and standards.[377] The Ministry of Economy participates in the "Cyberworld Awareness and Security Enhancement Structure", which makes recommendations and provides information on vulnerabilities and threats to the private sector, the national CERT, and the Computer Incident Response Center Luxembourg.[378] In addition, the CSIRT of the Réseau Téléinformatique de l'Éducation Nationale et de la Recherche specifically serves Luxembourg's research, educational, and cultural institutions.[379] Luxembourg has signed a memorandum of understanding with the Netherlands and Belgium for cooperation in cybersecurity, which includes information- and expertise-sharing, collaboration on best practices, and the development of public–private partnerships.[380]

Madagascar

Madagascar has worked to promote the development of ICT infrastructure through two key initiatives: the national ICT policy of 2004 and the Madagascar Action Plan for 2007–2012, both of which focus on economic and social development.[381] Madagascar refers to cybersecurity as "digital

376 European Network and Information Security Agency, *Luxembourg Country Report*, 2011, p. 5.

377 Luxembourg for Business, "Luxembourg Conference on Cybersecurity", 24 November 2011, www.investinluxembourg.lu/ict/luxembourg-conference-cybersecurity.

378 European Network and Information Security Agency, *Luxembourg Country Report*, pp. 10–11.

379 RESTENA CSIRT, "Welcome to RESTENA-CSIRT", www.restena.lu/csirt.

380 European Urban Knowledge Network, "Benelux sign memorandum of understanding on cybersecurity", 12 April 2011.

381 S. Isaacs, "ICT in education in Madagascar", *Survey of ICT and Education in Africa: Madagascar Country Report*, World Bank, 2007.

sovereignty". The government will work with the Southern African Development Community to harmonize cyber laws.

Maldives

The Maldives National Defence Force and the Police Service have called for a comprehensive cyber strategy and for cyber legislation.[382] With assistance from the US Federal Bureau of Investigation, the Maldives Police Service has started a project to investigate cybercrime.[383] The Maldives Police Service continues to develop its Cybercrime Department and a bill to legalize the Department's functions has been submitted to the Attorney General.[384] To date, Maldives has not enacted specific cybersecurity legislation. The government continues discussions with key public and private sector stakeholders on forming a national CERT.[385]

Malta

Malta's Information Technology Agency is responsible for implementing the National Strategy for Information Technology and is updating its CERT, which will become the central point of contact on cyberincidents and threats.[386] The Malta Police Force set up the Cybercrime Unit, which is responsible for investigating cybercrime and attacks on computer systems.[387]

---

382 A. Nazeer, "Dhiraagu attacks highlight Maldives' cyber crime challenge", *Minivan News*, 3 January 2011.

383 "Maldives Police Service launches cyber crime project", *Miadhu*, 20 May 2008.

384 "Development of Cyber-crime Department in progress", *Miadhu*, 26 June 2012.

385 International Telecommunication Union, *Readiness Assessment for Establishing a National CIRT (Afghanistan, Bangladesh, Bhutan, Maldives, and Nepal)*, 2012, pp. 37–40.

386 E. Darmanin, "National ICT Strategy and Malta Information Technology Agency", Malta Information Technology Agency, 3 June 2011, www.comnet.org.mt/wp-content/uploads/2011/06/MITA-Strategic-Plan-COMNET-Legal-Frameworks-for-ICT-Jun2011-v2.pdf; and European Network and Information Security Agency, *Malta Country Report*, 2011, p. 5.

387 P. Caruana, "Fighting cybercrime in Malta", Cyber Crime Unit Malta, www.terena.org/activities/tf-csirt/meeting13/Cyber-Crime-Malta-Caruana.pdf.

Mauritius

The National ICT Strategic Plan of 2011–2014 provides policy guidance for the development of infrastructure and services. Within the Ministry of Information and Communications Technology, the Central Information Systems Division ensures information security of government computer networks. Mauritius has established cybercrime laws,[388] including the Computer Misuse and Cybercrime Act of 2003[389] and the Fraud Tracking Account Charge Regulations of 2010.[390] Mauritius also has a national CERT that monitors and responds to computer security incidents, releases alerts with information about new threats, and recommends best practices and proactive security measures to public and private network operators.[391]

Mexico

The Mexican Public Security Secretariat has a police unit to investigate cybercrimes. The National Autonomous University of Mexico's CERT works with the Cybercrime Police to provide support and technical advice to Mexican authorities and shares data with information security professionals.[392] Mexico receives cybersecurity technical assistance through the OAS CICTE cybersecurity programme.

Mongolia

In March 2012, the Government Communications Department of the General Intelligence Agency was renamed the Cyber Security

388 K. Sikuka, "Southern Africa: region cracks down on cyber crime", *All Africa*, 12 April 2012.

389 "Republic of Mauritius", CyberCrime Law, 15 July 2003, www.cybercrimelaw.net/Mauritsius.html.

390 Government of Mauritius, *The Information and Communications Technologies Act 2001*, Legal Supplement of 2010, 5 August 2010.

391 "Mauritius Computer Emergency Response Team", www.gov.mu/portal/sites/cybersecurity/documents/Brochure CERT MU(F).pdf.

392 G. Diniz and R. Muggah, *A Fine Balance: Mapping Cyber (In)Security in Latin America*, Instituto Igarapé, 2012, pp. 13–14; General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General*, UN document A/64/129, 8 July 2009, pp. 7, 9.

Department.[393] It is responsible for providing security for the government and priority infrastructure, managing the government's information network, undertaking risk evaluations for the government and affiliate organizations, and establishing a network to transfer sensitive information through a secure network.[394] The Mongolian CIRT is a non-governmental organization.[395] Mongolia is a general member of APCERT, the Asia Pacific Computer Emergency Response Team. Mongolia's cooperation program with NATO includes a cybersecurity component.[396]

Montenegro

The Draft of the National Security Strategy adopted in 2008 mentions the need for improved information security due to vulnerabilities to cybercrime and terrorism.[397] In 2009, the government adopted the *Strategy for Information Society Development in Montenegro from 2009 to 2013* outlining specifically that "Defence and Security entities will build their own information-communication systems to satisfy specific requirements and commitments towards partners (NATO, etc)".[398] Montenegro has adopted a law on information security and set up a CIRT under the Ministry for Information Society and Telecommunications to manage security incidents.[399]

393 "Cyber Security Department to provide the security of the government organizations", *InfoMongolia.com*, 6 March 2012, www.infomongolia.com/ct/ci/3440/59.

394 Ibid.

395 APCERT Secretariat, *APCERT Annual Report 2011*, 2011, pp. 169ff.

396 NATO, "NATO and Mongolia agree programme of cooperation", 19 March 2012, www.nato.int/cps/en/natolive/news_85430.htm.

397 Montenegro Ministry of Defence, *Draft National Security Strategy*, 2008, pp. 7, 13, http://merln.ndu.edu/whitepapers/montenegro_National_Security_Strategy_English2008.pdf.

398 Montenegro Ministry for Information Society and Telecommunications, *Strategy for Information Society Development in Montenegro from 2009 to 2013*, 2009, p. 44, www.gov.me/files/1255505965.pdf.

399 Montenegro CIRT, "About us", www.cirt.me/en/about-us.

Morocco

Morocco's national strategy emphasizes cybersecurity as an economic benefit to ensure commerce and foster "cyber-confidence".[400] Previously, the Department of Post, Telecommunications, and New Technologies had developed a national cybersecurity programme in 2008.[401] The strategy recommends the creation of a committee for information systems security under the National Council of Information Technology and Digital Economy and the establishment of a national CERT. In 2011, Morocco established the Commission for Strategic Security of Information Systems and the General Directorate of Security of Information Systems to strengthen critical infrastructure protection and coordinate national efforts.[402] Morocco has cooperative cybersecurity agreements with the Republic of Korea[403] and with Malaysia.[404]

Nepal

In 2006, Nepal enacted the Electronic Transaction Act, known as the Cybercrime Law, intended to limit the unlawful use of the Internet and other e-platforms as Nepal continues to develop its use of information technology.[405] In 2010, the Nepali Police established the Communication, Information and Technology Crime Cell to help stop cybercrime.[406] The government also prepared a plan to form an Information Technology Emergency Response Team under the Ministry of Science and Technology to test and audit security of Nepali websites before putting them on the

400 Morocco Ministry, Trade and New Technologies, *Digital Morocco 2013: The National Strategy for Information Society and Digital Economy*, 2009, p. 22.

401 M. Jacob, "Le Maroc a préparé sa stratégie en matière de Cybersécurité", *Global Security Mag*, October 2009, www.globalsecuritymag.fr/Le-Maroc-au-coeur-de-la-lutte,20090930,12977.html.

402 "Le Maroc se dote de deux instances nationales de sécurité des systèmes d'information", *Hamza Security Blog*, 14 November 2011, www.hamza.ma/securite-news/le-maroc-se-dote-de-deux-instances-nationales-de-securite-des-systemes-dinformation.

403 "Morocco, South Korea to boost cooperation in ICT", *Morocco News Central*, 31 August 2009.

404 "Malaysia, Morocco partners in cybersecurity", *Malay Mail*, 27 January 2010.

405 See "A presentation on cyber crime in Nepalese perspectives", www.prp.org.bd/cybercrime_files/Cybercrime%20--%20Nepalese%20Perspective.ppt.

406 B. Sitaula, "Nepali Police forge ahead to curb cyber crime", *People's Daily Online*, 25 January 2010.

Internet. The International Telecommunication Union and a team of experts from the International Multilateral Partnership Against Cyber Threats carried out a readiness assessment of the cybersecurity situation in Nepal to review the institutional and regulatory framework and existing critical information infrastructure, identify areas of improvement, and make recommendations for establishing a national CIRT.[407]

New Zealand

New Zealand outlined its cybersecurity goals in its 2011 National Cyber Security Strategy. The strategy is divided into three priority areas: increasing awareness to promote online security, protection of online infrastructure, and computer emergency response. Its objectives are to raise understanding and awareness among small businesses and individuals, improve government cybersecurity, and improve cybersecurity in critical infrastructure.[408] The Ministry of Economic Development is the lead for cybersecurity policy. The National Cyber Security Centre under the Government Communications Security Bureau works with government agencies and critical infrastructure organizations to improve cybersecurity and protection against cyber threats. The Centre for Critical Infrastructure Protection has been subsumed under the National Cyber Security Centre.[409] Planning is underway to complement the Computer Emergency Readiness Team with a Computer Emergency Response Team. New Zealand's Unitec and Japan's National Institute of Information and Communications Technology established a new cybersecurity research centre in order to bolster New Zealand's cybersecurity.[410]

New Zealand's 2010 defence white paper discusses cyber attacks as a growing threat.[411] The New Zealand Defence Force's Statement of Intent

---

407 South Asian Telecommunications Regulators Council, *SATRC Report on Critical Information Infrastructure Protection and Cybersecurity*, adopted by the 13th meeting of the SATRC, 18–20 April 2012, Katmandu, Nepal, p. 29.

408 New Zealand Government, *New Zealand's Cyber Security Strategy*, 2011, p. 6.

409 New Zealand National Cyber Security Centre, "About NCSC", www.ncsc.govt.nz/about-us.html.

410 B. Chapman-Smith, "New research centre to boost NZ cybersecurity", *New Zealand Herald*, 25 September 2012.

411 New Zealand Ministry of Defence, *Defence White Paper 2010*, 2010, pp. 25, 41.

2011–2014 also discusses the threat of cyber attacks and says that New Zealand will increase support operations for its forces.[412]

Nigeria

In 2003, the National Cybersecurity Initiative was developed, which was implemented by the Nigeria Cybercrime Working Group and institutionalized in form of the Directorate of Cybersecurity under the Office of the National Security Advisor in 2006.[413] In 2007, the Directorate for Cybersecurity was established, responsible for internet-related security issues.[414] Nigeria is considering two pieces of cybersecurity legislation. The Harmonized Cyber Security Bill would criminalize hacking and create new legislative authorities for critical information infrastructure and international cooperation.[415] Another 2011 bill, still under consideration, would establish a Cybersecurity and Information Protection Agency.[416] Within the Office of the National Security Advisor, Nigeria has created a Directorate for Cybersecurity to update cyber policy and to coordinate efforts against cybercrime. Nigeria is again trying to pass a comprehensive cybercrimes bill after having failed to pass it six times since 2005.

Oman

The Information Technology Authority of Oman adopted an Information Security Framework to protect against unauthorized access and denial of service attacks.[417] The Authority promotes adherence to an Information

412 New Zealand Defence Force, *Statement of Intent 2011–2014*, pp. 12, 16.

413 M.U. Maska, "Building national cybersecurity capacity in Nigeria: the journey so far", presentation by the Director of Cybersecurity, Office of the National Security Advisor, Regional Cybersecurity Forum for Africa and Arab States, Tunis, 2009, www.itu.int/ITU-D/cyb/events/2009/tunis/docs/maska-nigeria-cybersecurity-june-09.pdf.

414 S. Badaru, "Nigeria: 419—FG okays N1.2b for Cybersecurity Directorate", *All Africa*, 6 April 2007.

415 E. Amaefule, "FG to present harmonised cyber security bill soon", *Punch*, 1 January 2012.

416 National Assembly of the Federal Republic of Nigeria, *Cybersecurity Bill 2011*, http://blogs.law.harvard.edu/mcash/files/2012/03/Nigeria-Cyber-Security-Bill-2011.pdf.

417 Information Technology Authority of Oman, "Security framework", www.ita.gov.om/ITAPortal/eServices/Popular_Projects.aspx?NID=89.

Security Management System in managing government and critical industry network information. Oman also created a national CERT in 2010.[418] Oman passed a law on cybercrime by royal decree in April 2011, which penalizes hacking and electronic fraud, as well as the dissemination of objectionable material.[419]

Pakistan

Pakistan passed the Prevention of Electronic Crime Act in 2009 to criminalize malicious computer activities. Two organizations were created to implement the law. The National Response Centre for Cybercrimes of the Federal Investigation Agency is responsible for preventing and investigating cybercrime, securing information resources, and providing information to departments and critical infrastructure owners about cyber threats.[420] The Centre, created in 2003, also gathers cybersecurity intelligence. PakCERT and CERT Pakistan assist in defending and responding to attacks against Pakistani organizations, and protecting information on online systems.[421] Some press reports suggest that the Interservices Intelligence Agency will create a special a cybersecurity unit.[422] The National Telecommunications and Information Technology Security Board (previously the National Communication Security Board) provides advice to the government and oversees purchases of IT equipment.[423]

Panama

Panama has criminalized cybercrime and the use of the Internet for terrorist purposes. The National Security Council, an intelligence organization, investigates the use of the Internet for terrorist purposes, and the Department of Law and Order within the Institute of Forensic

418 "Oman unveils cyber-security outfit", *Gulf News*, 5 April 2010.
419 Sultanate of Oman, *Royal Decree No. 12/2011 Issuing the Cyber Crime Law*, 11 April 2011.
420 See National Response Centre for Cybercrimes, www.nr3c.gov.pk.
421 See Pakistan Computer Emergency Response Team, www.pakcert.org.
422 "Exclusive—The ISI needs a special cyber wing?", *Pakistan Military and Defense News*, 30 August 2012, http://paksoldiers.com/intelligence/exclusive-the-isi-needs-a-special-cyber-wing.
423 M. Azam, "Cyber security regime in Pakistan, still a lot to be done!", *Propakistani*, 17 January 2011, http://propakistani.pk/2011/01/17/cyber-security-regime-in-pakistan-still-a-lot-to-be-done.

Medicine and Science investigates cybercrime. In 2011, the Incident Response Center for Cyber Security of Panama was established,[424] which houses the national CIRT.

Peru

In May 2012, the Peruvian government approved Ministerial Resolution 129-2012-PCM, which requires National Information System members to follow common information security standards.[425] Within the President's Council of Ministers, the National Office of Electronic Government and Information Technology is responsible for developing and implementing information security regulations.[426] The Office has established a national CERT.[427] Peru has participated in the OAS CICTE Cyber Security Program, and plans to establish a national CSIRT. Through this programme, Peruvian government ministries have received technical assistance to develop cybersecurity and CERT capabilities. Peru has reformed its penal code to incorporate crimes committed using information technology.[428] The National Police has a High Technology Crimes Investigation Division, which is responsible for investigating crimes committed using information and communications technology.[429]

Philippines

In January 2012, the Philippines passed the Cybercrime Prevention Act to "define and penalize internet-related crimes and empower law enforcement agencies in the investigation and prosecution of cyber criminals". The Act created the Office of Cybercrime under the Department of Justice, the National Cyber Security Center under the Department of Science and

424 K. Gómez, "Workshop Panama Prevention Headquarters Cyber Security Incident", RED GEALC, 24 November 2011.

425 Republic of Peru, *Resolución Ministerial No 129-2012-PCM*, 23 May 2012.

426 Peru National Office of Electronic Government and Information Technology, "Quienes somos", www.ongei.gob.pe/quienes/ongei_QUIENES.asp.

427 See Peru National Office of Electronic Government and Information Technology, www.peru.gob.pe/pecert/label.html.

428 J. Gamba, *Panorama del derecho informático en América Latina y el Caribe*, United Nations Economic Commission for Latin America and the Caribbean, 2010, pp. 23–24, 26.

429 High Technology Crimes Investigation Division, National Police of Peru, "Misión, visión y valores", www.policiainformatica.gob.pe/nosotros.html.

Technology, and the National Cybersecurity Coordinating Council under the Office of the President. The Supreme Court recently postponed the implementation of the Cybercrime Prevention Act for 120 days in order to hear arguments on the law's constitutionality.[430][431]

The Philippines' Task Force for the Security of Critical Infrastructure issued the first National Cyber Security Plan in 2005. The Plan called for reducing vulnerabilities, nurturing a culture of cybersecurity among individual users and critical sectors, and strengthening self-reliance on information technology and human resources.[432] The Task Force also created the National Cyberspace Security Coordination Center, tasked with detecting and investigating computer network intrusions and incidents.[433] In 2008, the National Cybersecurity Coordination Office was established by the Commission on Information and Communication Technology in the Office of the President and an undersecretary appointed as National Cybersecurity Coordinator.[434]

The Cybersecurity Works Group serves as the advisory body to the National Cybersecurity Coordination Office and includes members of the National Security Council, Philippine National Police, National Bureau of Investigation, Department of Justice, Armed Forces of the Philippines, and National Computer Center. It implements national cybersecurity policy and collaborates with the private sector, local governments, non-governmental organizations, and international partners in enhancing cybersecurity.

The Armed Forces of the Philippines has announced plans to create an operations centre to handle cybersecurity threats.[435]

---

430 D. Kerr, "Philippines court halts a contentious cybercrime law", *CNET*, 9 October 2012.

431 A.A. Saludar, "Cyber crime prevention act passes 3rd reading in Senate", Philippine Information Agency, 31 January 2012.

432 Philippines National Cybersecurity Coordination Office, "Philippine cybersecurity efforts", 2010, p. 44, www.itu.int/ITU-D/asp/CMS/Events/2010/NGN-Philippines/S5-Philippines_cybersecurity.pdf.

433 Ibid., p. 48.

434 Ibid.; V.V. Gil, National Cybersecurity Coordinator, *National Cyber Security Efforts*, presentation at the Armed Forces of the Philippines Summit on Enhancing Cybersecurity, National Cyber Defence Capability Development Conference, Manila, 10–11 March 2010.

435 E. Phneah, "Philippines to set up cybersecurity operations center", *ZDNet*, 19 November 2012.

Portugal

Portugal's Knowledge Society Agency is tasked with developing a national cybersecurity strategy.[436] Portuguese cyber legislation covers computer-related exploitation and includes provisions to protect critical information infrastructure.[437] The Judicial Police force includes a unit specialized in cyber- and information-related crime, known as the Central Investigations Section for IT and Telecommunications,[438] and the Minister for Home Affairs said that Portugal will create a special cybersecurity centre responsible for investigating cybercrime.[439] The Security Intelligence Service has a cybersecurity mission that includes investigating organized cybercrime, ensuring the security of critical networks, and preventing the use of the Internet to incite violence, radicalization, and terrorism.[440]

Qatar

Cybersecurity in Qatar falls under the Supreme Council of Information and Communication Technology, established in 2004. A national CERT was created in 2005. The National ICT Plan commits the CERT to developing strategies and policies to protect critical infrastructures and other government systems.[441] It carries out these tasks in part through its National Information Assurance Framework project, whose steering committee comprises key operators of critical infrastructure. The Framework is Qatar's main thrust towards a comprehensive national cybersecurity strategy, as it aims to identify key actors and their responsibilities.[442] The Office of

436 Knowledge Society Agency, "R&D in cybersecurity", 24 October 2011, www.english.umic.pt/index.php?option=com_content&task=view&id=3415&Itemid=187.

437 General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General, Addendum*, UN document A/66/152/Add.1, 16 September 2011, pp. 6–7.

438 European Network and Information Security Agency, *Portugal Country Report*, 2011, pp. 5–8, 22.

439 "Cybersecurity centre to open in Portugal", *PRLog*, 8 March 2012.

440 Portugal Security Intelligence Service, "Ciberameaça", www.sis.pt/ciberameaca.html.

441 Qatar Supreme Council of Information and Communication Technology, *National ICT Plan 2015: Advancing the Digital Agenda*.

442 M. Lewis, "Q-CERT: National Cybersecurity Strategy—Qatar", presentation at ITU Regional Cybersecurity Forum for Asia–Pacific and Seminar on the

Internet Security and Intelligence is in charge of monitoring governmental and national networks to address threats to the state.[443]

In 2010, the Ministry of Interior formed a committee to draft cybercrime legislation, aiming to align Qatari law with the Convention on Cybercrime. The draft has been completed,[444] but the law has not yet been passed by Parliament. The penal code does, however, cover criminal cyber activity. Cybercrime cases are handled by the Cybercrime Unit in the Ministry of the Interior, with support from the CERT.[445] With the cooperation of the National Police of the Republic of Korea, a Cybercrime Prevention Center was set up in 2009 under the Criminal Investigation Department at Capital Security, one of several regional cybercrime centres that Qatar plans to establish.[446]

Republic of Moldova

The Republic of Moldova's National Security Concept recognizes cyber threats and identifies the need to strengthen cybersecurity.[447] The Ministry of Information Development is the lead ministry regarding information and

Economics of Cybersecurity, Brisbane, Australia, 15–18 July 2008, www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/lewis-qatar-national-strategy-brisbane-july-08.pdf.

443 General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General*, UN document A/65/154, 20 July 2010, p. 9.

444 Qatar Supreme Council of Information and Communication Technology, *National ICT Plan 2015: Advancing the Digital Agenda*.

445 Qatar Supreme Council of Information and Communication Technology, "Qatar progresses in cyber crime prevention measures", 17 April 2012.

446 Qatar Ministry of Interior, "Electronic Crimes Prevention Centre inaugurated", www.moi.gov.qa/site/english/news/2009/12/27/21345.html.

447 Moldova Ministry of Foreign Affairs and European Integration, *National Security Concept of the Republic of Moldova*, www.mfa.gov.md/img/docs/national-security-concept-of-the-RM.doc; Moldova National Participation Council, "National Security Strategy went into force", 17 October 2011, www.cnp.md/en/working-groups/foreign-security-and-defense-policy/stiri/item/568-strategia-securit%C4%83%C8%9Bii-na%C8%9Bionale-a-intrat-%C3%AEn-vigoare.

communications technology and is in charge of establishing "e-Moldova, a plan to digitize government operations".[448]

Romania

Romania's Service for Countering Cyber Criminality is responsible for preventing and investigating cyberattack. It is part of the Directorate for Countering Organized Criminality.[449] The National Security Strategy mentions cyberterrorism[450] and the national CERT serves as a hub for information security and promoting awareness of potential cyber threats.[451]

Rwanda

Rwanda is currently expanding its cybersecurity capabilities. The Rwanda Utilities Regulatory Agency is leading efforts to draft a national ICT bill that will address cybersecurity. The strategic plan developed by the Agency would create a National Cyber Security Research Center.[452]An additional goal of the strategic plan is to set up a national CSIRT, which will cooperate with other teams at the regional and the international level.[453]

448 Moldova Ministry of Defence, *Concepției reformei militare*, 15 August 2002, http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=307788.

449 UK Trade and Investment, "Cyber security in Romania", 23 October 2012, www.ukti.gov.uk/export/sectors/creativemedia/fashion/sectorbriefing/393840.html.

450 Romania Ministry of National Defence, *Romania's National Security Strategy*, http://mercury.ethz.ch/serviceengine/Files/ISN/15286/ipublicationdocument_singledocument/ad89b866-fe51-4987-b293-221be20c0453/en/ROMANIA.pdf.

451 See www.cert-ro.eu/?lang=en.

452 J. Rugondihene, "The issue of cyber security and the level of preparedness in Rwanda", Rwanda Utilities Regulatory Agency, www.rura.gov.rw/EACO/Presentations/Regulators_Assembly/Cybersecurity_rwanda-EACO%20Congress%20final.ppt.

453 D. Nkurikiyimfura, "Rwanda cyber briefing: positive steps and challenges", 2011 East African Internet Governance Forum, 17 August 2011, www.eaigf.or.ke/files/Rwanda_Cybersecurity_briefing_EAIGF_2011.ppt.

Saint Vincent and the Grenadines

Saint Vincent and the Grenadines has outlined a national strategy for cybersecurity in an appendix of the National ICT Strategy and Action Plan 2010–2015 developed by the Ministry for Telecommunications, Science, Technology and Innovation. This plan has specific goals such as appointing a lead official and lead institution for the national effort, improving government–industry collaboration, deterring cybercrime, developing incident management capabilities, and developing a culture of cybersecurity, and offers specific methods of achieving each of these goals.[454] In 2007, Saint Vincent and the Grenadines passed the Electronic Transactions Act designed to counter cybercrime and provide the framework for protecting information systems. The Act also identifies "cyber inspectors", whose job is to investigate possible infringements of the law and cooperate with law enforcement to apprehend criminals.[455]

Saint Vincent and the Grenadines also participated in the Workshop on Best Practices in Cyber-Security and Cyber-Crime, where OAS members discussed cybercrime persecution mechanisms and national cybersecurity strategies.[456]

Saudi Arabia

Saudi Arabia has a national CERT concerned primarily with awareness-raising, incident management, and threat analysis.[457] The Saudi Armed Forces also has a special Internet Services Center, whose objectives include ensuring the security of military systems and providing consulting services for the military. The Center's Department of Network Operations aims to

454 Saint Vincent and the Grenadines Ministry for Telecommunications, Science, Technology and Innovation, *National Information and Communication Technology Strategy and Action Plan 2010–2015*, 2010, pp. 103–105, www.carib-is.net/ictpolicies/st-vincent-grenadines-national-ict-strategy-and-action-plan.

455 The Act is available at www.oas.org/juridico/spanish/cyb_svg_electronic_act_2007.pdf.

456 OAS, "Saint Vincent and the Grenadines to participate in workshop on best practices in cyber-security and cyber-crime", 28 November 2011, www.oas.org/en/about/offices_events.asp?sCode=STV.

457 Saudi Arabia Computer Emergency Response Team, "CERT-SA services", www.cert.gov.sa/index.php?option=com_content&task=view&id=186&Itemid=131.

protect servers and communication systems and provide technical support, while the Department of Network Security protects confidentiality of information.

In 2007, Saudi Arabia passed the Anti-Cybercrime Law, penalizing acts of hacking and electronic fraud, as well as electronic dissemination of information undermining public morality or supporting terrorist organizations. The Law tasks the Bureau of Investigation and Public Prosecution with enforcement and the Communications and Information Technology Commission with technical support.[458]

Serbia

The National Security Strategy of Serbia cites the increased use of information and computer technology in the military and in society as promoting efficiency and coordination. Serbia opened its Cybercrime Department in 2005, which specializes in cybercrime court cases. It became operational in 2007, overseeing the judicial process for cybercrime prosecution throughout the country. The Republican Agency for Telecommunications plays a leadership role in internet regulations and information security issues. Regulations entitled "Instructions for Technical Requirements for Subsystems, Devices, Hardware and Installation of Internet Networks" establish privacy and security standards for internet service providers and producers of hardware and software.[459] The police have expanded the organized crime department to handle cybercrime. In addition, the Criminal Code has been changed to add cybercrime, and the judiciary has formed new departments that specialize in cybercrime.[460]

Slovenia

Slovenia's National Security Strategy emphasizes the dangers of cyber risks and the misuse of information technologies as a significant risk to national

458 Kingdom of Saudi Arabia, Bureau of Experts at the Council of Ministers, *Anti-Cyber Crime Law (8 Rabi 11428 / 26 March 2007)*, 1 August 2010, www.saudiembassy.net/announcement/announcement03260701.aspx.

459 "Serbian telecom agency publishes internet traffic interception laws", *EDRI-Gram*, 30 July 2008.

460 "Dacic advocates cooperation against cyber crime", *Tanjug*, 13 September 2012.

security.[461] The military acknowledges the electromagnetic spectrum as one of the five dimensions of future war.[462] Slovenia will develop a national strategy to respond to these threats, which will emphasize domestic measures and will establish public–private partnerships and a national coordinating body. The Computer Investigation Centre within the Criminal Police Directorate proposed the creation of a National Cyber Security Center to work with government ministries and the national CERT to increase information dissemination.[463]

Sudan

Sudan has established a CERT under its National Telecommunications Corporation. The CERT seeks to provide early warning and first response services, guidance for constituent parties, protection of critical infrastructure, and support for cybercrime investigations.[464]

Swaziland

The Government Computer Services Department in the Ministry of Information and Communications Technology has the mission to maintain reliable networks and the security of government data.[465] The key goal of the Ministry is to build ICT infrastructure in the country.

461 Slovenian Ministry of Defence, *Resolution on the National Security Strategy of the Republic of Slovenia*, 2010, pp. 14, 16–17, www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/pdf/ministrstvo/RSNV2010_slo_en.pdf.

462 Slovenia Doctrine, Development, Education and Training Command, *Military Doctrine*, 2006, p. 89, www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/pdf/ministrstvo/vojd2006_eng.pdf.

463 T. Kastelic, "National Cybersecurity Center—Slovenia", Slovenia Computer Investigation Centre, Criminal Police Directorate, http://elivinglab.org/CrossBordereRegion/DeRc/Presentations/Kastelic_CyberSecurity.pdf.

464 Sudan Computer Emergency Response Team, "About us", www.cert.sd/index7bd7.html?option=com_content&view=article&id=82&Itemid=37.

465 Swaziland Ministry of Information, Communication and Technology, "Computer services", <www.gov.sz/index.php?option=com_content&view=article&id=331&Itemid=398.

Sweden

Sweden's Civil Contingencies Agency, which succeeded the Emergency Management Agency in 2009, is responsible for national information security and ICT incident response.[466] In 2011, the Agency released an interim draft of the National Response Plan for Serious IT Incidents, which emphasized cooperative approaches with industry and other agencies to minimize disruption. The Response Plan will be implemented pending exercises to be carried out by the end of 2012.[467] Other agencies with cybersecurity responsibilities participate in the Cooperation Group for Information Security, established in 2003. These include the Post and Telecom Agency, the Defence Materiel Administration, and National Defence Radio establishment, the Armed Forces/Military Intelligence and Security Service, the Security Service, and the Criminal Investigation Service.[468] In 2011, the Civil Contingencies Agency established the National Cybersecurity Coordination Function as a forum for situational awareness and collaboration.[469] It focuses on prevention and coordinates incident response. It will also work closely with the armed forces to protect confidential information.[470] The Strategy to Improve Internet Security in Sweden appeared in 2006.[471]

Syrian Arab Republic

In 2011, the Syrian Arab Republic established the Information Security Center within the National Agency for Network Services. The Center has three divisions—a department of computer systems security, a department of network security, and a CERT—and aims to develop the policies and

466 Swedish Civil Contingencies Agency, *Measures to Improve Sweden's Ability to Prevent and Handle IT Incidents*, 13 January 2010.

467 Swedish Civil Contingencies Agency, *Handling Serious IT Incidents: National Response Plan, Interim Version*, March 2011, 2011.

468 Swedish Civil Contingencies Agency, *Cooperation Group for Information Security (SAMFI)*, 2012.

469 Swedish Civil Contingencies Agency, *Handling Serious IT Incidents: National Response Plan, Interim Version*, March 2011, 2011.

470 European Network and Information Security Agency, *Sweden Country Report*, 2011, pp. 2–6.

471 Swedish Post and Telecom Authority, *Strategy to Improve Internet Security in Sweden*, 4 July 2006.

capabilities to combat cybercrime, and to detect, analyse, and manage cyber threats.[472]

Thailand

Thailand's national CERT operates under the National Science and Technology Development Agency. The CERT is a member of APCERT.[473] In April 2012, Thailand signed a memorandum of cooperation with Symantec to create a national cybersecurity system.[474] The Information and Communications Technology Ministry will create a National Cyber Security Policy Committee to revise the Cybercrime Law and the E-Transaction Law in order to support the development of a new national cybersecurity policy framework that will tackle online crime and fraud.[475]

Trinidad and Tobago

Trinidad and Tobago is developing a National Strategy for Cyber Security under the direction of an interministerial committee led by the Ministry of National Security. The committee's mandate includes developing a cyber strategy action plan, making recommendations for cybercrime legislation, planning the enforcement of cybersecurity regulations, assessing the vulnerabilities of national infrastructure, and creating a national CSIRT.[476]

Tunisia

In 2004, Tunisia established the National Agency for Computer Security under the Ministry of Information and Communications Technologies

472 Syrian National Agency for Network Services, "Information Security Center (ISC)", http://nans.gov.sy/index.php/isecurity.

473 Thailand Computer Emergency Response Team, "About us", www.thaicert.or.th/about-en.html.

474 T. Kunakornpaiboonsiri, "Thailand to set up national cyber security system", *Asia Pacific FutureGov*, 30 April 2012.

475 J. Bonnoon, "ICT Ministry plans cyber-security framework", *The Nation*, 3 February 2012.

476 Ministry of National Security of Trinidad and Tobago, "Formal opening of the Roundtake Talks of the Trans-Border Expert Alliance for Caribbean Security", 5 October 2010.

as well as a CERT.[477] The national CERT falls under the authority of the Agency, which is tasked with ensuring the security of public and private systems, except those of the Ministries of Defence and of Interior.[478]

Uganda

Uganda's 2010 Information Technology Policy called for the development of a National Information Security Strategy and the establishment of a National Information Security Working Group and a national CERT.[479] The CERT was established under the Communications Commission in 2012 and monitors online activity for cyber fraud, cyberterrorism, and online sexual exploitation.[480] In March 2011, the Ministry of Information and Communications Technology released a final draft of the National Information Security Strategy, which outlines the state's strategic objectives, including the protection of critical information infrastructure.[481] The Strategy also defines current information technology threats to include cybercrime, cyberwarfare, and cyber terrorism.[482] Uganda has three laws to provide the legal framework for to prosecute cybercrime and cyberterrorism.[483] The government has also participated in regional cybersecurity efforts, such as the US Department of State-sponsored East Africa Workshop on cyberspace security and East African Community efforts to develop a cyber law framework.[484]

---

477 Family Online Safety Institute Global Resources Information Directory, "Tunisia", www.fosigrid.org/africa/tunisia.

478 Tunisian National Agency for Computer Security, "Legal frame", www.ansi.tn/en/about_agency/cadre_juridique_en.html.

479 Uganda Ministry of Information and Communications Technology, *Information Technology Policy for Uganda*, February 2010.

480 "Uganda deploys special unit to fight cyber crime", *IT News Africa*, 14 August 2012.

481 Uganda Ministry of Information and Communications Technology, *National Information Security Strategy*, 2011.

482 Ibid., pp. 7–10, 24–27.

483 See National Information Technology Authority Uganda, www.nita.go.ug/index.php/policies-and-laws/cyber-laws.

484 US Department of State, "East Africa cyber workshop to address cyber security", 22 July 2011; East African Community Secretariat, *Third Meeting of the EAC Task Force on Cyberlaws (Phase II). Report of the Meeting*, document EAC/TFCL/ /3/2011, October 2011, http://r0.unctad.org/ecommerce/docs/EAC_report.pdf; and A. Harris, S. Goodman, and P. Traynor, "Privacy and security

United Arab Emirates

In September 2011, the United Arab Emirates launched a cyber operations centre in Abu Dhabi.[485] The centre is a joint effort between the firm Emiraje Systems and Khalifa University and will coordinate with the armed forces.[486] The first phase of the United Arab Emirates Command and Control System was completed in February 2011. There is a national CERT, established by the Telecommunications Regulatory Authority in 2008. It currently serves as the state's cybersecurity coordination centre.[487] In 2006, a law on cybercrime was passed, penalizing acts of hacking, electronic fraud, and the dissemination of objectionable materials.[488] The United Arab Emirates enforces cybercrime law via its Anti-Cybercrime Directorate under the Directorate General for Criminal Investigations.

United Republic of Tanzania

The government of the United Republic of Tanzania recognizes the danger from cybercrime and established a Cybercrime Unit in the National Police Force with a specialized team of investigators trained in cybercrime investigation and a response centre. Additionally, the Office of the Attorney General, Division of Public Prosecution, coordinates cybercrime investigation and prosecution, reviews proposed laws, and provides guidance to law enforcement on cybercrime. While the United Republic of Tanzania has not drafted specific cybercrime legislation, the government is using existing communications laws to regulate cybercrime while drafting additional measures. Further, there is an initiative to

concerns associated with mobile money applications in Africa", *Washington Journal of Law, Technology and Arts*, vol. 8, no. 3, 2013.

485 "Khalifa University opens Cyber Operations Centre of Excellence in Abu Dhabi in collaboration with Cassidian and Emiraje Systems", Khalifa University, 19 September 2011.

486 "Cassidian, Emiraje and Khalifa University complete the first phase of establishing Cyber Operations Centre of Excellence", *MENA Business News Network*, www.menann.com/article/cassidian-emiraje-and-khalifa-university-complete-first-phase-establishing-cyber-operations.

487 "DP World UAE region signs MoU with CERT to reinforce information security", *AMEinfo*, 12 April 2011.

488 United Arab Emirates Computer Emergency Response Team, *The Federal Law No. (2) of 2006 on the Prevention of Information Technology Crimes*, 30 January 2006, www.aecert.ae/preventionoftechcrimes.php.

establish a national CERT under the Electronic and Postal Communications Act of 2010. In 2012, a Cybercrime Unit and a CERT were established. The United Republic of Tanzania participates in regional efforts to develop common cybersecurity legislation through the African Union, East African Community, and Southern African Development Community.[489]

Uruguay

Uruguay has a CSIRT, a CERT, and the Agency for the Development of Government Electronic Management and Information Society and Knowledge. Uruguay is a member of the Inter-American Integral Strategy to Combat Threats to Cyber Security.[490] The government hosted the Regional Cyber Security and Cybercrime Best Practices Workshop under the auspices of the OAS in July 2012.

Yemen

Yemen is in the process of developing cybersecurity capabilities. Though it does not currently have a CERT, a special unit for cybercrime has reportedly been established under the Ministry of Interior.[491] The National Information Center handles cybersecurity insofar as it proposes new cybersecurity policies, ensures adherence to those policies, and maintains backups of government systems.[492]

Zimbabwe

According to the 2010–2014 Strategic Plan prepared by the Ministry of Information Communication Technology, Zimbabwe intends to create a cyber policy, which would be implemented and monitored by Ministry

489 S.M. Kalunde, "The status of cybercrime in Tanzania", presented at the Octopus Conference on Cooperation Against Cybercrime, www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/Octopus2011/Update_session_Tanzania.pdf.

490 See www.oas.org/en/about/offices_detail.asp?sCode=URU.

491 United Nations Economic and Social Commission for Western Asia, *Regional Profile of the Information Society in Western Asia*, 2011, p. 59, http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan049096~1.pdf.

492 International Telecommunication Union, *ICT Adoption and Prospects in the Arab Region*, 2012, p. 134.

through 2013.[493] Zimbabwe launched the IT Governance and Cyber Security Institute of Sub-Sahara in early 2012. Its mandate is to increase information exchange, promote research and reporting of cyber threats, and hold periodic ICT security symposiums.[494]

493 Zimbabwe Ministry of Information Communication Technology, *Strategic Plan 2010–2014*, www.techzim.co.zw/wp-content/uploads/2010/02/zimbabwe_mict_strategic_plan2010-2014.pdf.

494 IT Governance and Cybersecurity Institute for Sub-Saharan Africa, "About us", http://itgcsinstitute.co.zw/home1.html.

CHAPTER 2

ASSESSMENT OF INTERNATIONAL AND REGIONAL ORGANIZATIONS AND ACTIVITIES

Götz Neuneck

With the growth and expansion of the Internet and related information and communications technologies (ICTs) there is an emerging international concern regarding the potential use of cyberattack during conflict and war. While a pure cyberwar is highly unlikely, future armed conflicts or skirmishes might be increasingly accompanied by the disruption of digital networks and services. Additionally, massive attacks on the Internet and/or critical infrastructure of states potentially could trigger conventional counterattacks.[495] Despite the fact that many key questions about terminology, feasibility, rationale, and motivation of potential cyberattacks are not yet answered sufficiently, the international debate about the future challenges and possible legal, technical, and political reactions of the international community to those challenges has begun. In 2010, a United Nations Group of Governmental Experts, including diplomats from China, the Russian Federation, and the United States, stated in its consensus report, "Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century".[496]

Many states are now developing national strategies to implement safer and more secure digital infrastructures. Some argue that humankind is entering "a new era of warfare";[497] others believe that militarization of the cybersphere is looming, including new kinds of cyberweapons.[498] It is often argued by military thinkers that cyberspace is becoming the "5th battlefield", after land, sea, air, and space. Others take a more subtle view:

495 P. Sommer and I. Brown, *Reducing Systemic Cybersecurity Risks*, OECD document IFP/WKP/FGS(2011)3, 2011.

496 General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Document A/65/201, 30 July 2010, p. 6.

497 K. Benedict, "Stuxnet and the bomb", *Bulletin of the Atomic Scientists*, 15 June 2012.

498 J.A. Lewis and K. Timlin, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*, UNIDIR, 2011.

that while cyberweapons might be new sorts of weapons, there is little difference between cyberweapons and other types of weaponry. In any event, militaries around the world seem to be rushing to incorporate both defensive and offensive cyber options as part of their operational toolkits for warfighting. Thus, strategies to prevent the misuse of the cybersphere are now being considered in many national, regional, and international forums.

Although debate about cyber and national/international security remains at an early stage, different stakeholders can already been seen to be favouring different strategies. The most direct measures for governments to take include the improvement of security standards of national critical information infrastructures through cooperation with the public and private sectors. Another national approach would be to improve civil preparedness for contingency planning, as well as to implement best practices and training of operators, and raise the awareness of individual citizens. However, national strategies are not enough. Given the global access to digital technology and the worldwide structure of the Internet, international cooperation will be a key factor in preventing future cyberconflict. Governments, the private sector, and civil society must work together to coordinate national efforts, legal and regulatory approaches, and international responses to prevent future cyber threats.

International conferences and meetings on cyberspace sponsored by governments and international organizations are taking place frequently to bring together a wide range of stakeholders to discuss political, technical, educational, and legal responses to cyber challenges. The spread of ICTs and networking technologies is also a cross-dimensional issue, which—beyond technical development—has human, political, cultural, and legal dimensions that affect many societies. Also, several aspects of the problem overlap significantly: cybercrime and cyberterrorism, the protection of critical information infrastructure and information networks, the preservation of fundamental human rights, and the emergence of "cyberweapons" as part of the military arsenal. Various obstacles also have to be overcome in addressing these aspects, for example the dual-use character of modern ICTs, the open nature and the fast-growing use of the Internet, different cultures of communication, competing interests among stakeholders, and national differences regarding threat perceptions.

ROLE OF INTERNATIONAL ORGANIZATIONS

Some studies have already been undertaken to address the function, role, and activities of international organizations in the cyberspace field.[499] International efforts to address cyber threats are, in comparison to national strategies, more limited in terms of resources. Most international organizations now active in the cyber domain are intergovernmental, founded and influenced by governments, and based on multilateral treaties. The most prominent example is certainly the United Nations, which has near global state participation and outreach. The International Telecommunication Union (ITU) is another key international body. Regional organizations such as the Organization of American States (OAS), the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF), the Asia–Pacific Economic Cooperation Organization, and the Organization for Security and Co-operation in Europe (OSCE) also play important roles.

While most of the concrete work on cyberdefence is organized by states, international organizations can discuss, coordinate, and develop proposals to enhance global strategies for the creation of appropriate regional and international structures, institutions, and policies. This spectrum of work ranges from establishing/strengthening norms and principles to prevent the malicious use of new cybertechnologies, to brokering of agreements about the application of the law of armed conflict, to promoting national prevention of, preparation for, response to, and recovery from cyberincidents. For these purposes, international organizations have the power to bring together the most relevant actors in the cybersecurity domain—governments, the private sector, civil society, and individual citizens.

United Nations

The United Nations General Assembly has approved a number of resolutions relevant to ICTs and cybersecurity that have served to draw the attention of United Nations Member States to future cyber challenges. A

499 H.I. Touré, "The international response to cyberwar", in H.I. Touré, *The Quest for Cyberpeace*, ITU and World Federation of Scientists, 2011, pp. 86–103; European Parliament, Directorate-General for External Policies, Policy Department, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*, 2011, p. 20.

recent study underlined the emerging norm-building process within the United Nations system.[500] Several specialized United Nations agencies are dealing with cybersecurity on different levels. The United Nations Office on Drugs and Crime supports the United Nations by addressing illicit drug control and crime prevention, including through the cyber domain. The World Customs Organization, which facilitates global supply chain security, is active in promoting strategies for critical infrastructure protection. The United Nations Economic and Social Council is focusing on improved information exchange, best practices, and training to fight the criminal misuse of information technology.[501]

The issue of telecommunication and information security has been on the United Nations agenda since the Russian Federation in 1998 first introduced a draft resolution (A/35/576, 18 November 1998) in the First Committee of the General Assembly, which was adopted as resolution 53/70 in January 1999 without a vote.

The General Assembly adopted in 2003 and 2004 two resolutions dealing with the creation of a "Global Culture of Cybersecurity and the Protection of Critical Infrastructures". Resolution A/57/239 of 2003 calls for more awareness and responsibility by capable states to "act in a timely and cooperative manner to prevent, detect and respond to security incidents".[502] Resolution A/58/199 of 2004 invites all relevant international organizations and Member States "that have developed strategies to deal with cybersecurity and the protection of critical information infrastructures to share their best practices and measures that could assist other Member States in their efforts to facilitate the achievement of cybersecurity".[503] In 2010 and 2011, the United Nations Secretary-General released annual reports to the General Assembly with the views of Member States on new developments in the field of information in the context of international

500 T. Maurer, *Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security*, Belfer Center for Science and International Relations, 2011.

501 General Assembly, *Combating the Criminal Misuse of Information Technologies*, UN document A/RES/56/121, 23 January 2002.

502 General Assembly, *Creation of a Global Culture of Cybersecurity*, UN document A/RES/57/239, 31 January 2003, p. 2.

503 General Assembly, *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*, UN document A/RES/58/199, 30 January 2004, p. 2.

security.[504] In particular, the report of 2011 (A/66/152) includes long statements by Australia, Germany, the Netherlands, and the United States regarding transparency and confidence-building measures (TCBMs).

In addition, there have been two groups of governmental experts (GGE) established to discuss and examine the existing and potential threats stemming from activities in the cybersphere. GGEs are convened by the Secretary-General at the request of the General Assembly to explore areas of special concern. They consist of no more than 15 members nominated by their national governments, and work by consensus. In 2004, the GGE failed to reach agreement. The second GGE was convened in 2009 with the mandate "to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them".[505] A report was issued in 2010, calling for "further dialogue among States to discuss norms pertaining to State use of information and communications technologies (ICTs), to reduce collective risk and protect critical national and international infrastructure". It also recommended "Confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict".[506] The GGE worked out a useful agenda for future work based on norms, TCBMs, and capacity-building. However, states remain divided on several key questions, such as can certain types of information be defined as "weapons", and do the law of armed conflict and international humanitarian law apply to the cybersphere?

In 2010, the General Assembly approved a resolution (A/RES/65/41) calling for a follow-up to the 2009 GGE. This new GGE started its work in August 2012, to continue the study of existing and potential threats in the sphere of information security and identify possible cooperative measures to address them, taking into account the assessments and recommendations contained in the 2010 report. This GGE will report to the sixty-eighth session of the General Assembly in September 2013. It is believed that the

504 General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/65/154, 20 July 2010; General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/66/152, 15 July 2011.

505 General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/65/201, 30 July 2010, p. 5.

506 Ibid., p. 8.

next step will be "to develop some specifics on what the implementation of the recommendations might look like and—equally importantly—designate a forum for discussion of TCBMs in cyberspace".[507]

On 12 September 2011, the permanent representatives to the United Nations of China, the Russian Federation, Tajikistan, and Uzbekistan submitted a letter to the Secretary-General asking for discussions of a draft proposal for an International Code of Conduct for Information Security in the framework of the United Nations. This draft model contains basic principles for maintaining information and network security. Under the proposed code, each subscribing state would pledge "Not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, and pose threats to international peace and security or to proliferate information weapons and related technologies".[508]

International Telecommunication Union

The ITU is a specialized United Nations agency for regulating telecommunications and use of the radio frequency spectrum. The ITU has been seeking to expand its remit to include cybersecurity, not without some tensions among its member states about what the limits should be to its involvement, particularly in political questions of international peace and security. It has 193 members from the public and private sectors, including ICT regulators, academic institutions, and some 700 companies. Since its founding in 1865, the ITU has played a major role in setting standards in telecommunication security. The ITU consists of three sectors: the Radiocommunication Sector, the Standardization Sector, and the Telecommunication Development Sector. It is the only intergovernmental organization within the United Nations system embracing all actors in the ICT domain. The ITU is currently working on cybersecurity issues through a range of activities related to standardization and technical assistance, as well as to developing technical guides for critical infrastructure protection,

507 B. Baseley-Walker, "Transparency and confidence-building measures in cyberspace: towards norms of behavior", *Disarmament Forum*, no. 4, 2011, p. 37.

508 General Assembly, *Letter Dated 12 September 2011 from Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, UN document A/66/359, 14 September 2011, p. 4.

botnet mitigation, and training development for developing countries. An ITU High-Level Expert Group on Cybersecurity was founded in 2007 as a consultation platform for information security experts from various domains and regions. On 17 May 2007, the ITU launched the Global Cybersecurity Agenda "to provide a framework within which all stakeholders can coordinate an international response to the growing challenges in cybersecurity" and "to build confidence and security in the information society".[509] The Agenda is built on five pillars: legal measures, technical procedures, organizational structures, capacity-building, and international cooperation.[510] The ITU also collaborates with the International Multilateral Partnership Against Cyber Threats, which focuses on early warning systems and a secure electronic collaboration platform for coordination of incident response measures, and the Forum for Incident Response and Security Teams, which is an international confederation of trusted computer incident response teams (CIRTs) that cooperatively handle computer security incidents and promote incident prevention programmes. The Forum also accredits computer emergency response teams (CERTs) worldwide. The Agenda continues to form partnerships for different stakeholders and seeks to enable states to implement concrete measures for cybersecurity.

Internet governance organizations

The Internet as a new global infrastructure for communication and business was created as an open "bottom up" medium for free speech and the exchange of information. From the beginning, internet governance groups have played an important role by self-regulating and promoting new internet applications. According to a 2011 European Union study, organizations can be divided into the technical and the political domains.[511]

Governments, which are "latecomers" in the dynamic and volatile internet world, are supportive but not central in these "bottom up" institutions. Thus, these groups have a significant role to play in technical questions

509 H.I. Touré, *The Quest for Cyberpeace*, ITU and World Federation of Scientists, 2011, p. 104.

510 See www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf.

511 European Parliament, Directorate-General for External Policies, Policy Department, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*, 2011, p. 20.

of cybersecurity, but they have not as yet been directly influential on questions of international security and military use. On the other hand, the political debate among governments about the extent of national sovereignty in the cybersphere in recent years has started to spill over to these venues.

Technical groups such as the Internet Engineering Task Force or the Institute for Electrical and Electronics Engineers are developing and discussing software protocols, connectivity, and electronic standards.

The non-profit, private Internet Corporation for Assigned Names and Numbers (ICANN) oversees vital internet-related tasks such as assigning names and internet addresses, ensuring its stable and secure operation. The United States government, which helped to establish ICANN in 1998, still has significant influence on the Government Advisory Council that gives advice to ICANN on issues of public policy, especially where there may be an interaction between ICANN's activities or policies and national laws or international agreements. Approximately 50 governments and distinct economies, global organizations (such as the ITU and the United Nations Educational, Scientific and Cultural Organization), and regional organizations (such as the Organization for Economic Co-operation and Development, the Asia Pacific Forum, and the Council of Europe) attend three meetings a year. In the cybersecurity field, informal internet governance initiatives also exist, such as the Meridian Forum for Global Critical Infrastructure Protection, which is an important trust-building and consultation forum.

Slightly afield from these technical organizations but concerned with the same issues is the Internet Governance Forum, a multi-stakeholder forum for facilitating dialogue. It was created by the United Nations Secretary-General in 2006, and first convened in Athens the same year. The group holds annual meetings, as well as workshops and consultations, to help articulate issues such as internet development of resources, ensuring access for all, and maintaining security.

Convention on Cybercrime

The 2004 Budapest Convention on Cybercrime of the Council of Europe is the only international binding treaty on cybercrime.[512] It serves as a

512 See http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

guide for states to develop national legislation on cybercrime and as a framework for international cooperation. The Convention laid out general principles for international cooperation on cybercrime, especially between internet service providers and law enforcement agencies. Cybercrimes such as hacking and data interception are specifically addressed in the Convention.[513] It states that cyberattacks are illegal, regardless of their motivation. It does not focus on other cyberattacks such as espionage or sabotage, although there is an overlap between cybercrime, cyberterrorism, and cyberwar, both from a technological view point and with regard to actors. The Convention requires signatories to establish a basic legal framework to address cybercrime. It also forms a basis for cooperation in the case of a severe cyberincident. However, only 37 states have ratified the treaty. While most European states have ratified the Convention, the Czech Republic, Greece, Ireland, Luxembourg, Poland, Sweden, and Turkey have not. Outside of Europe, only Japan and the United States have ratified. The Council of Europe holds annual conferences in Strasbourg and supports states in implementing the Convention, as it is considered "a useful tool for 'exporting' European norms on the issue". The Council and the private sector have launched the Global Project on Cybercrime to promote broad implementation of the Convention and related international standards.[514]

Group of Eight

The Group of Eight is an international forum of the governments of Canada, France, Germany, Italy, Japan, the Russian Federation, the United Kingdom, and the United States. In 2011 in Deauville, France, these states for the first time discussed and agreed on a number of principles the must be upheld in order to underpin a stable and flourishing Internet, such as freedom, respect, privacy, protection of intellectual property, multi-stakeholder governance, cybersecurity, and prosecution of crime. In addition, the Group maintained that "non-discrimination and fair competition", as well as "flexibility and transparency", are key aspects of the multi-stakeholder approach required to protect the Internet in the future. The Deauville Declaration underlines that "Governments have a

513 The Convention includes technical and legal definitions of various forms of cybercrime.

514 See www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project%20global%20phase%202/projectcyber_en.asp.

role to play, informed by a full range of stakeholders, in helping to develop norms of behaviour and common approaches in the use of cyberspace".[515] The main goal of the Group of Eight is to establish a sharing mechanism among leading industrialized nations to prevent, investigate, and prosecute cybercrimes. To this end a special forum was held in Paris on 24–25 May 2011. A subgroup worked on the protection of critical information infrastructure and cybercrime, and created a network for points of contact in more than 50 countries. This work could be expanded by follow-up discussions in the Group of 20 framework.

Key international conferences

In November 2012, the United Kingdom hosted the London Conference on Cyberspace, designed to launch a high-level political dialogue on cyber issues and set the agenda for further work to build a secure, resilient, and trusted global digital environment. The two-day conference concentrated on five themes: economic growth and development, social benefits, cybercrime, safe and reliable access, and international security. Its goal was to provide "a structured non-formal forum in which … the next steps for further action and discussion can be agreed".[516] A follow-up was held in Budapest in October 2012, which gathered nearly 600 representatives of governments, the private sector, civil society, and the scientific community, as well as international journalists.[517] The next in this series of international conferences is planned for 2013 in Seoul.

"Challenges in Cybersecurity", held in December 2011 in Berlin, was sponsored by the German Federal Foreign Office, UNIDIR, the University of Hamburg's Institute for Peace Research and Security Policy, and the Free University of Berlin. The meeting brought together key stakeholders and decision makers from civil society, the private sector, academia, and governments to explore challenges to international security in the cyber domain and potential multilateral solutions, including the establishment of TCBMs, such as greater transparency in defence doctrines, better mechanisms for crisis management, improved law enforcement

515 Deauville G8 Declaration, *Renewed Commitment for Freedom and Democracy*, 2011, p. 6.

516 B. Baseley-Walker, "Transparency and confidence-building measures in cyberspace: towards norms of behavior", *Disarmament Forum*, no. 4, 2011, p. 35.

517 See www.cyberbudapest2012.hu.

cooperation, and shared understanding on the application of the law of armed conflict to cyberattacks.[518]

UNIDIR, in partnership with the Verification Research, Training and Information Centre and Chatham House, also held a two-day multinational conference in November 2012, specifically on the potential of TCBMs in building and ensuring stability and security in the cyber domain. This conference also took a multi-stakeholder approach, seeking to highlight areas of mutual interest as well as areas of competing interests. A follow-up conference is planned for 2013.

REGIONAL ORGANIZATIONS

Traditionally, regional intergovernmental organizations have proven powerful forums for building security, in particular by developing and implementing cooperative security arrangements and confidence-building measures (CBMs). Firstly, regional approaches have the advantage of involving fewer states, but with related interests. Secondly, agreement to and implementation of specific measures is sometimes easier at the regional level than at the global level, especially in regions with highly-developed cooperative arrangements and experienced existing institutions.

Organization of American States

The OAS, which originated in 1889 and which today includes all 35 independent states of the Americas, formed a Group of Governmental Experts on Cybercrime to analyse criminal activities related to computer networks, compare national legislation, and identify national and international entities with relevant expertise. In 2004, the OAS General Assembly approved resolution 2004 XXXIV-O/04, The Inter-American Integral Strategy to Combat Threats to Cybersecurity, and provided a mandate to the Inter-American Committee against Terrorism (CICTE) to begin working on cybersecurity. The CICTE Secretariat created a cybersecurity programme and established national computer security incident response teams (CSIRTs).[519] At the fourth plenary session of the

518 *Challenges in Cybersecurity: Risks, Strategies, and Confidence Building*, Institute for Peace Research and Security Policy at the University of Hamburg, 2011, http://unidir.org/pdf/activites/pdf2-act667.pdf.

519 OAS, "Cyber security program", www.oas.org/en/sms/cyber.

OAS on 7 March 2012, the member states approved the Declaration on Strengthening Cyber Security in the Americas, which called for the development of national cyber strategies and strengthening international cooperation mechanisms. In August 2012, CICTE presented in Washington, DC, a "Mobile Simulation Laboratory" designed to train member state personnel, and conducted a simulation exercise on critical infrastructure protection. The Laboratory will be available to all member states for further training, and exercises will include participation of the private sector, governments, and civil society. Additionally, a Regional Cyber Dialogue of the OAS members is planned to begin a conversation on principles of behaviour in the cybersphere.

Organization for Security Co-operation in Europe

The OSCE is an ad hoc, regional organization under the Charter of the United Nations created during the Cold War, which offers a regional forum for high-level dialogue with a comprehensive view on security that combines the politico-military, economic, environmental, and human dimensions. With 57 participating states, the OSCE is the largest security-oriented regional intergovernmental organization, covering most of the northern hemisphere including North America, Europe, and the Russian Federation—from "Vancouver to Vladivostok". Its mandate includes topics such as early warning, conflict prevention, crisis management and post-conflict rehabilitation, arms control, and the promotion of human rights, freedom of the press, and fair elections. The Secretariat, the Permanent Council under rotating chairmanship that is the OSCE's political decision-making body, and the Forum for Security Cooperation are located in Vienna. At the Forum, the participating states discuss and take decisions regarding military and arms control issues within the OSCE area, in particular CBMs. The Vienna Documents and the Treaty on Conventional Armed Forces in Europe showcase a rich toolbox of approved CBM and transparency measures in the field of conventional forces. The OSCE forums provide venues for continuous dialogue and negotiation.

In 2008, the OSCE started discussing cybersecurity issues by holding several high-level meetings, and in May 2011 there followed the OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role. On 26 April 2012, the OSCE Permanent Council approved at its 909th Plenary Meeting a decision on development of CBMs to reduce the risks of conflict stemming from the use of ICTs, which establishes an open-ended, informal working group "To elaborate

a set of draft [CBMs] to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs; To help build consensus for the adoption of such a set of CBMs in 2012; [and] To provide progress reports … and preliminary proposals on possible CBMs".[520] The advantage of the OSCE is its comprehensive and cross-dimensional focus based on its foundational commitments and tradition of cooperation. The OSCE held its nineteenth Ministerial Council on 6–7 December 2012 in Dublin, at which cybersecurity and CBMs were debated. In particular, a new measure requiring governments to provide pre-notification of activities in the cyber arena that may spark concern or unintentional conflict failed due to lack of consensus.[521]

European Union

The 2008 European Council's Report on Implementation of the European Security Strategy included cyber threats as a new risk to European security.[522] The European Union is active in two cybersecurity areas that overlap significantly: measures to combat cyberattacks including cybercrime, and measures to support critical infrastructure protection and network security. As relates to cyber issues, the Common Foreign and Security Policy is underdeveloped—"in part due to its confidential and interdepartmental nature, but also due to the difficulties in approaching the subject perceived to be a matter often left to Member States" according to a European Parliament study.[523]

The first key documents about the protection of network and information systems date back to 2005. A new EU Internal Security Strategy was adopted in October 2010 to raise the level of cybersecurity for all

520 Permanent Council, *Decision No. 1039: Development of Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, OSCE document PC.DEC/1039, 26 April 2012.

521 A. Sternstein, "Cyber early warning deal collapses after Russia balks", *NextGov*, 7 December 2012.

522 European Council, *Report on Implementation of the European Security Strategy: Providing Security in a Changing World*, EU document S407/08, 11 December 2008.

523 European Parliament, Directorate-General for External Policies, Policy Department, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*, 2011.

EU citizens and businesses. This includes the establishment of an EU Cybercrime Centre in 2013, a CERT network including all EU institutions by 2012, and the launch of the European Information Sharing and Alert System by 2013. The institutions and agencies have different areas of responsibility. The Directorate-General Home Affairs deals with cybercrime and related legislation. An information-sharing platform for member states has been in existence since 2009. Pan-European cybersecurity exercises and functional CERTs are planned to be established in all EU member states by the end of 2012 to protect Europe from large-scale cyberattacks.

The European Union's approach to critical information infrastructure protection was triggered by the 2007 cyberattacks on Estonia. The European Commission's Directorate-General Information Society and Media published several documents for an infrastructure protection initiative at that time.[524] The Directive on Attacks Against Information Systems attempts to harmonize the legal framework to combating cybercrime. The Directorate-General is creating an information-sharing platform for EU member states, including European public–private partnerships. The European Network and Information Security Agency was established in 2004 as a research and advisory body for EU member states and institutions, but its mandate to address, respond to, and especially to prevent network and information security problems was extended and is still under review.[525] The Agency is financed and supervised by the Directorate-General Information Society and Media and will also be responsible for the European Information Sharing and Alert System.

Cybersecurity is also an integral part of the European Common Foreign and Security Policy (CFSP), but it is less developed compared to the cybercrime and critical information infrastructure protection activities. CFSP falls also under the mandate of the European External Action Service. The Service will, as a next step, focus on the development of norms and standards for cyberspace, the promotion of the Convention on Cybercrime, capacity-building in third states, development of a European strategy for cyberspace, and the organization of joint workshops with India and China, and the North Atlantic Treaty Organization (NATO). The European Union Institute

524 European Parliament, Directorate-General for External Policies, Policy Department, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*, 2011, p. 33.

525 European Network and Information Security Agency, "About ENISA", www.enisa.europa.eu/about-enisa.

for Security Studies seminar "Cyber Security: What Role for CFSP?" was held in 2009 to discuss foreign policy ramifications of CFSP.[526] An occasional paper by the Institute states that European military authorities are also discussing the feasibility of developing a European common doctrine for computer network operations.[527] In 2011, "Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU", a comprehensive study done at the request of the European Parliament Committee on Foreign Affairs and the Subcommittee on Security and Defense, examined policy options for EU institutions and member states to strengthen cooperation on cybersecurity.

The European Union plays an important role in setting and discussing norms and debating resilience measures to support member states. However, in terms of technical, legal, and political harmonized measures, there are still significant differences between individual member states and EU institutions. Despite its civilian orientation, the European Union is nevertheless an important player in relation to the United States and security organizations within Europe, such as NATO and the OSCE.

Shanghai Cooperation Organization

The Shanghai Cooperation Organization (SCO) was founded in 2001 by China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan, which encompasses 60 per cent of the Eurasian land mass. The SCO holds a summit once a year and cooperates in the area of security, economics, and culture, and has initiated several large-scale projects related to energy, communication, and transportation. Several states, including India, the Islamic Republic of Iran, and Pakistan, participate as observers, and Belarus, Sri Lanka, and Turkey are dialogue partners since 2008. In September 2011, the SCO released an "Agreement on Cooperation in the Field of Information Security",[528] which is seen by the members as the basis of further discussion within the United Nations. The agreement lists in article 2 as a main threat, "the development and use of information weapons, preparing and waging information war" and the

526 J.-P. Zanders, *Institute Report. Seminar on Cyber Security: What Role for CFSP?,* European Union Institute for Security Studies, 10 March 2009.

527 L. Simón, *Command and Control? Planning for EU Military Operations*, occasional paper no. 81, European Union Institute for Security Studies, 2010.

528 See http://media.npr.org/assets/news/2010/09/23/cyber_treaty.pdf.

"use of the dominant position in the information space to the detriment of the interests and security of other states".[529] Information threats are described in the agreement as "Dissemination of information harmful to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other states". Other dangers such as "information terrorism" and "information crime" are also mentioned as threats. The SCO agreement also contains in annex I a list of basic terms such as "information war", "information weapon", and "critical structures". Also, as mentioned above, on 12 September 2011, China, the Russia Federation, Tajikistan, and Uzbekistan submitted to the United nations Secretary-General a draft proposal based on their regional agreement for an "International Code of Conduct for Information Security" in the framework of the United Nations.[530]

ASEAN Regional Forum

The ASEAN Regional Forum is a multilateral dialogue organization, consisting of 27 participating states, founded in 1994 to foster constructive dialogue, consultations, and cooperation primarily in the field of political relations and security in the Asia–Pacific region.[531] The ARF is active in discussing and implementing confidence-building and preventive diplomacy. The member states are cooperating in combating cyber threats. In 2006, the participating states issued the "ARF Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space".[532] The main focus was criminal and terrorist misuse of cyberspace. The "Workshop on Proxy Actors in Cyber Space" was held in Viet Nam in March 2012 emphasizing development of some specifics on how to implement the agreed guidelines, and equally important, designate a forum for discussion of TCBMs in cyberspace to expand the ARF role in the cyber field.[533] At

529 Ibid., annex 2, item 1.

530 General Assembly, *Letter Dated 12 September 2011 from Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, UN document A/6/359, 14 September 2011.

531 ASEAN Regional Forum, "About the ASEAN Regional Forum", http://aseanregionalforum.asean.org/about.html.

532 See www.mofa.go.jp/%5Cregion/asia-paci/asean/conference/arf/state0607-3.html.

533 "Co-chairs' summary report", ARF Workshop on Proxy Actors in Cyberspace, Hoi An City, Viet Nam, 14–15 March 2012, http://aseanregionalforum.

the nineteenth ARF meeting in Phnom Penh, Cambodia, on 12 July 2012, the ministers adopted the "Statement on Cooperation in Ensuring Cyber Security". In particular, ARF states agreed to intensify cooperation by developing joint strategies to overcome cyber threats. They also declared their intent to promote dialogue on confidence-building "to reduce the risk of misperception, escalation and conflict". Additionally, they pledged to close the "digital divide" by investing in capacity-building for less-developed ARF states. States such as Australia, China, and the United States are active in implementing national cybersecurity strategies and addressing these issues in the ARF context.[534]

North Atlantic Treaty Organization

NATO is the largest military alliance in the world with regard to military expenditure, weapon systems, and high-tech equipment. Its mandate is restricted to collective defence and crisis management in the North Atlantic area. NATO started its Cyber Defence programme in 2002 after denial-of-service attacks in the late 1990s during the Kosovo war.[535] At the 2002 Prague summit, NATO leaders decided to launch the NATO Computer Incident Response Capability, which is responsible for responding to cyberattack against NATO computer networks. The Coordination Centre in Brussels and the Technical Centre in Mons are dealing with unauthorized intrusions, prevention measures, and digital forensics, and offer support to member states. They are part of the NATO Communication and Information Services Agency. In 2008, the Cooperative Cyber Defence Centre of Excellence (CCDCOE) was established in Tallinn, Estonia, to conduct research, education, and training and to host workshops on legal, doctrinal, and technical cyberwarfare issues.[536] One important focus is on the development of a legal framework. The Centre invited a group

asean.org/files/library/ARF%20Chairman%27s%20Statements%20and%20Reports/The%20Nineteenth%20ASEAN%20Regional%20Forum,%202011-2012/10%20-%20Co-Chairs%20Summary%20Report%20-%20ARF%20Workshop%20on%20Proxy%20Actors%20in%20Cyberspace,%20Quang%20Nam.pdf.

534 Directorate for ASEAN Political and Security Cooperation, *ASEAN Regional Forum Annual Security Outlook–2011*, 2011, pp. 15ff.

535 For details see, S. Myrli, *NATO and Cyber Defence*, NATO document 173 DSCFC 09 E bis, 2009, para. 45.

536 NATO Cooperative Cyber Defence Centre of Excellence, "About", www.ccdcoe.org.

of independent international experts to examine how international law, norms, and practices are applicable to cyberwarfare. After three years, a draft version of the so-called "Tallinn Manual" was published and is open for further discussion.[537] The CCDCOE also serves as an interface between academia, the private sector, and the military. It organizes training events and workshops and has a large outreach mission, including cooperation with the European Union.

NATO also created the Cyber Defence Management Authority (CDMA) to coordinate and initiate "immediate and effective cyber defence action if appropriate". A NATO Parliamentary Assembly report says, "On request, the CDMA is also prepared and able to co-ordinate or provide assistance in a concerted effort if an Ally or Allies fall victim to a cyber attack of national or Allied significance".[538] NATO officials further revealed the development of Rapid Reaction Teams to be made available for immediate deployment in an emergency to counter cyberattack on the request of member states.[539] Requests from non-member states have to be approved by the NATO Council. NATO hosts annual cyber exercises on defence of attacks on NATO computer infrastructure.

NATO has signed cybersecurity memorandums of understanding with Estonia, the United States, the United Kingdom, Turkey, and Slovakia. NATO also conducts dialogue with industrial partners in the framework of the Trans-Atlantic Defence Technological and Industrial Cooperation, which is a part of the future "Smart Defence" project. A list of practical recommendations for cooperation was released in a research paper of the NATO Defense College.[540]

On 8 June 2011, NATO Defence Ministers approved a document with the revised NATO policy on cyberdefence, a classified document that defines NATO's cyberdefence efforts, and an associated action plan for its implementation. In October 2011, ministers agreed on details for the action plan. The new Strategic Concept adopted at the Lisbon Summit in November 2010 underlines that NATO should accelerate its efforts "to

537 NATO Cooperative Cyber Defence Centre of Excellence, "The Tallinn Manual", www.ccdcoe.org/249.html.

538 S. Myrli, *NATO and Cyber Defence*, NATO document 173 DSCFC 09 E bis, 2009, para. 52.

539 Ibid., para. 56.

540 V. Joubert, *Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO?*, research paper no. 76, NATO Defense College, 2012.

develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations".[541]

Debates continue about how NATO should react to cyberattack especially in relation to article V of the North Atlantic Treaty, which states that "an armed attack against [an Alliance member or members] shall be considered an attack against them all". First, it is still unclear whether a cyberattack can be judged as so severe that it could be legally determined as an "armed attack". The new Strategic Concept states that cyber attacks "can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability". The notion of an armed attack was not addressed, however, in the Strategic Concept, which instead merely references "collective defence". Second, NATO members are divided about what would constitute an appropriate response to such an attack: Is deterrence by punishment the right answer? Are offensive cyber missions effective and feasible? Will conventional strikes be considered?

Despite organizational and technical efforts, NATO is still continuing to refine its cyberdefence policy to secure and protect NATO's computer networks, and to encourage and support its member states to build robust national cybersystems. NATO, however, has no mandate to deal with civilian cybersecurity issues. International cooperation with other key multilateral organizations, such as the European Union, the OSCE, and ITU, could, however, be organized in a complementary way to meet the cyber challenges of the Euro–Atlantic societies. Better preparedness to prevent cyberincidents, early warning, exchange of technical expertise, and common work on the legal framework are important fields for cooperation.

541 North Atlantic Treaty Organization, "Active engagement, modern defence", www.nato.int/cps/en/SID-4EEB2033-B2ABB368/natolive/official_texts_68580.htm.

PART II

TRANSPARENCY AND CONFIDENCE-BUILDING MEASURES: APPLICABILITY TO THE CYBERSPHERE?

Götz Neuneck

In contemplating multilateral approaches to reducing risks of conflict in the cybersphere, policymakers confront a number of complex problems. Unlike in traditional arms control and confidence-building, the focus cannot be on "weapons", military forces, or government/military-controlled assets and facilities, due to the dual-use, and largely civilian owned, infrastructure of the domain. In addition, the integration of the global economy into the cyber domain makes state-based regulatory control somewhat difficult. Nonetheless, as cyberspace becomes increasingly a tool for militaries and for state-sponsored activities such as espionage and the dissemination of propaganda, there is widespread agreement that boundaries on some activities, and measures to reduce the risk of conflict, must be found at the multilateral level. However, the debate at this stage remains undeveloped, as states continue to hold competing and often contradictory views about legal obligations, threats, what constitutes an attack, and appropriate/responsible responses to threats or attacks. For example, most Western states believe that freedom of access to the cybersphere is a basic human right, which must be protected by law and regulations. Other states, in contrast, favour the concept of "information security", and thus are seeking the right to limit the access of their citizens to the public cybersphere if the stability or survival of the regime is deemed to be at stake. Obviously, these two ideological approaches are in direct conflict, and complicate the effort to find multilateral solutions to the problems that face all states.

Nonetheless, a spectrum of preventive and crisis-management strategies to secure the cybersphere for different stakeholders already can be envisioned. At the substate level, strategies should obviously include raising awareness, and the improvement of security standards for individual computers, servers, and networks. Making national critical information infrastructure more robust and resilient can only be achieved in cooperation between the public and private sectors. Governments and industry can strengthen civil preparedness for contingency planning as well as offering best practices and training for operators. Early warning and quick reaction is of upmost importance should a massive cyberattack occur. Just as obviously, given the interconnected nature of the cybersphere, states will need to

work together to ensure cybersecurity, as many threats, such as cybercrime or cyberterrorism, know no boundaries. However, there is a lack of a central international mechanism for discussing strategies—rather there is a plethora of potential forums all, with different focuses. This is proving another obstacle for state-based efforts to establish norms, common security standards, and ways to adapt or strengthen existing regulations, law enforcement, and information-sharing.

Due to the growing concerns about the potential for the use of cybertools to spark conflict and even traditional warfare, there are nascent efforts within the United Nations and the Organization for Security and Co-operation in Europe (OSCE), and among like-minded states, to identify practical transparency and confidence-building measures to avoid miscalculations or misperceptions regarding the use of the cyber domain. As noted, in 2010, a United Nations Group of Governmental Experts reached agreement on five general recommendations for future actions, among them "Further dialogue among States to discuss norms pertaining to State use of ICTs [information and communications technologies], to reduce collective risk and protect critical national and international infrastructure", and, in particular, "Confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict".[542]

The first chapter explores the dimensions of the problem, including the challenges to and opportunities for a secure and stable cyberspace. The second chapter refers to classical concepts of confidence-building developed during the Cold War and applied to different weapon systems, including nuclear, conventional, and space weapons, as well as in non-military fields such as disaster relief. The third chapter compares how traditional types of trust and confidence-building measures (TCBMs) could or could not be applied in the cyber domain.

542 General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Document A/65/201, 30 July 2010, para. 18.

CHAPTER 1

CIVILIAN AND MILITARY CYBERTHREATS: SHIFTING IDENTITIES AND ATTRIBUTION

Götz Neuneck

The characteristics of the global cyber domain include low barriers of technological entry, minimal technical skills required of the individual user, and rapid dissemination, replication, and exchange of all forms of data all over the world, which has lead to an unprecedented global connectedness.[543] In his seminal report, Joseph Nye described the key characteristics of cyberspace and the implications for foreign policy: "The low price of entry, anonymity, and asymmetries in vulnerability means that smaller actors have more capacity to exercise hard and soft power in cyberspace than in many more traditional domains of world politics".[544] A closer look at current cyberincidents reveals that different forms of cyberconflict with changing motivations and actor categories are emerging.[545]

Increasingly, organized global cybercrime using sophisticated cyber technology (for example, botnets) is a concern for states. Terrorist organizations have so far only used the cybersphere to recruit followers and to organize fundraising, but there is no guarantee that will remain the limits of their activities. "Hacktivist" groups such as Anonymous and LulzSec are challenging corporations, institutions, and governmental agencies whose policies or actions the hackers dislike.

In the West, there are constant rumours that "cyber warriors" supported by state entities are systematically attacking governments. Following revelations about Stuxnet, worms and trojans such as Flame, Duqu, and Gauss have been discovered, revealing that sophisticated espionage

543 J.B. Sheldon, "Achieving mutual comprehension: why cyberpower matters to both developed and developing countries", *Disarmament Forum*, no. 4, 2011, p. 43.

544 J.S. Nye, Jr., *Cyber Power*, Belfer Center for Science and International Affairs, 2010, p. 1. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

545 See D.J. Betz and T. Stevens, *Cyberspace and the State. Toward a Strategy for Cyber-Power*, International Institute for Security Studies, 2011, pp. 16–34.

programmes using cybertools are being actively applied, especially in the Middle East. In most cases the origin of such malware is unclear: are these efforts state-sponsored or private activities? What are the motivations and resources behind these incidents? Are states preparing for cyberwar?

Types of actors also vary widely. "White Hat" hackers, or "ethical" hackers, exploit computer systems for enjoyment or—when employed by an organization—to reveal security gaps. "Black Hat" hackers, however, break into computer systems for personal gain. Cybercriminals include thieves who steal personal data or charge bank accounts illegally, but also those who threaten to do so to extort money from the private sector. The differentiation among these categories is thin and fluctuating, but very often the tools being used are the same. A 2011 study sponsored by the European Parliament concluded that, "Most cyberthreats involve elements of loosely connected networks and actors with rapidly shifting identities, whereas government responses tend to take place within preexisting institutional settings".[546]

STATES AS ACTORS: PREPARING FOR CYBERWAR?

Strong assertions have been made by security companies and academics about future cyber threats that could be caused by, and directed against, states. For some, cyberwar is already real, and is capable of devastating modern countries. Former National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism for the United States Richard A. Clarke wrote that cyberwar "has already begun as nations prepare the battlefield … [by] hacking into each other's networks and infrastructure".[547] The internet security company McAfee warned in 2012 that a "cyber arms race" is developing based on a survey of 250 leading authorities worldwide. It said that 57 per cent of global experts believe that an arms race is taking place in cyberspace.[548] On the other hand, a 2011 Organisation for Economic Co-operation and Development (OECD) study dismissed such doomsday visions because in order to effect massive disruption or damage

546 European Parliament, Directorate-General for External Policies, Policy Department, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*, 2011, p. 5.

547 R.A. Clarke, *Cyberwar: The Next Threat to National Security and What to Do About It*, 2010, p. 30–31.

548 B. Grauman, *Cyber-Security: The Vexed Question of Global Rules*, 2012, Security and Defence Agenda, 2012.

to national infrastructures, highly orchestrated attacks would be required, based on unprecedented levels of preparatory work, coordination, and resources.[549]

Nonetheless, governments increasingly perceive cyber threats to be rapidly on the rise and that future cyberconflict between states might become a reality. If cyberattacks cause massive damage, the conflict might escalate, leading to a full-fledged armed conflict. Without doubt, many states are now implementing military cybercapabilities.[550] As noted earlier, this study has identified six states with explicit military cyber strategies, two more with pending military cyber strategies, and 30 which identify cybersecurity as a military priority. James Lewis has explained that already military doctrines of some states include "the use of cyber capabilities for reconnaissance, information operations, the disruption of critical networks and services, for cyber attacks, and as a complement to electronic warfare and information operations".[551] His analysis concludes that "only a few major 'Cyber Powers' have the capability to use software commands sent over the Internet to cause physical destruction". However, he points out that a number of states are developing military capabilities, and that "non-state actors will gain this capability as techniques and tools are commoditized".[552]

Obviously, militaries around the world must protect their own critical infrastructure against attack from the outside. It is thus completely understandable that national militaries are seeking strategies to defend assets and networks; what is unclear is how those strategies can be crafted so as not to imperil international security and stability. What is even less clear is how the advent of offensive cybertools for use in warfare will affect international stability, crisis escalation, warfighting, civilian infrastructure, and the global economy.

Unfortunately, many questions about "cyber-enabled" conflict are still unanswered: Under what conditions will military cybertools be deployed and used? Will this lead to escalation or de-escalation in times of crisis?

---

549 See P. Sommer and I. Brown, *Reducing Systemic Cybersecurity Risk*, OECD, 2011.

550 See J.A. Lewis and K. Timlin, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*, UNIDIR, 2011.

551 J.A. Lewis, "Confidence-building and international agreement in cybersecurity", *Disarmament Forum*, no. 4, 2011, p. 51.

552 Ibid., pp. 51–52.

Who will be responsible for any damage and how will an adversary react? What is the meaning of self-defence, offence and defence in the cybersphere? Under what conditions can cyberattack be labelled an "armed attack" and trigger conventional conflict? Will future wars and military campaigns be accompanied by attacks via the Internet?

Currently, there is disagreement among policymakers, military thinkers, and legal scholars about what might constitute cyberwar, which is relevant for trying to predict future state behaviour. "Strategic cyberwarfare" can be seen as complementary to classical warfare, similar to air power, which can be used to strike at the heart of a country by attacking its critical infrastructure. However, there is little agreement about what exactly would constitute a strategic cyberattack. For example, where is the line drawn between cybersabotage and cyberattack?

In addition, militaries are now relying much more on computer systems and networks for day-to-day operations, and using assets in the public and private domains due to the dual-use character of ICTs and digital network technologies. Does this make the cyber domain ripe for more "tactical" warfighting? Does it make public/private assets legitimate targets?

The developing nature of the current situation exacerbates the many obstacles to the development of multilateral agreements to shape responsible state behaviour in the cybersphere.[553] States may not be willing to forgo the possibility of using cyberattacks, described by some as "cheap" and "bloodless", because of the strategic advantages they may offer. Regarding limitations and restraint, it is highly unclear which, if any, offensive cyber operations could be prohibited. Cybertechnologies are widely available commercial products and therefore very difficult to control. Further, state activities regarding military cybercapabilities typically are surrounded by secrecy, thus making multilateral dialogue difficult. Lewis correctly concludes: "The combination of a high degree of secrecy and weak research methodology complicate policymaking".[554]

Another key challenge, both for military planning and for efforts to develop constraints, is to identify the originator of any specific cyberattack. Malign cybertools are either commercially available or "homemade", and the computers used and the origins of algorithms can be obscured. Consequently, one of the greatest challenges for "arms control in

553 Ibid., p. 57.
554 Ibid., p. 55.

cyberspace" is the attribution of an attack to a government, institution, location, or a specific person. Ben Basely-Walker concludes: "Even if the perpetrator is identified in a timely fashion with a high degree of confidence, proving an act was state-sponsored is extremely challenging and often impossible".[555]

Lewis concludes:

> Cyberconflict is shaped by covertness, ease of acquisition and uncertainty, and a legally binding convention that depends upon renouncing use, restricting technology, or upon verification of compliance is an unworkable approach for reducing the risk to international security from cyber attacks. An effort to secure an overarching cybersecurity agreement or treaty that attempted to address the full range of cybersecurity issues would be impractical.[556]

555 B. Baseley-Walker, "Transparency and confidence-building measures in cyberspace: towards norms of behavior", *Disarmament Forum*, no. 4, 2011, p. 33.

556 J.A. Lewis, "Confidence-building and international agreement in cybersecurity", *Disarmament Forum*, no. 4, 2011, p. 58.

CHAPTER 2

TYPES OF CONFIDENCE-BUILDING MEASURES

Götz Neuneck

Confidence-building measures (CBMs) have been used for decades to achieve better conditions and relations for a reliable peace between states. Depending on different conflict areas, political, economic, environmental, or societal CBMs are conceivable. They can build trust and confidence between different conflicting actors in politics, the administration, the military, or within other societal groups. CBMs aim to change threat perceptions in order to transform state relations and behaviour for conflict prevention, better crisis management, and conflict resolution. CBMs must be tailored to the context and the field of application in which they have to be implemented. The key characteristics of CBMs and measures related to the success of CBMs are reciprocity, transparency, predictability, and reliability.

If CBMs are related directly to the military and security domains, they are called confidence- and security-building measures (CSBMs). In the framework of treaties, they can be politically and legally binding. They can be unilateral, bilateral, or multilateral. They are aimed at preventing the outbreak of violent conflict and have been elaborated and implemented in a systematic way during and since the end of the Cold War.[557] Practical examples are on-site inspections or notification of military activities. Given a general level of mistrust and suspicion between states especially in the military sector, transparency and confidence-building measures (TCBMs) are politically binding instruments aimed at reducing threats, building trust between states, and making relationships between actors more reliable and predictable. They can help to prevent miscalculations of military activities, which could lead to war or unnecessary arms build-ups.[558] Often CBMs and TCBMs are seen as a point of entry for and a bridge to future legally binding agreements. CBMs cannot per se solve conflicts, but they

557 See for example the *OSCE Guide on Non-Military Confidence-Building Measures (CBMs)*, 2012.

558 B. Baseley-Walker, "Transparency and confidence-building measures in cyberspace: towards norms of behavior", *Disarmament Forum*, no. 4, 2011, p. 32.

can lay out the basis to improve relations between states and to create the preconditions for conflict resolution.

That said, the lines between CBMs, CSBMs, and TCBMs are somewhat blurred and the terms are often used interchangeably—adding to some confusion regarding the precise categorization of any such tool. Nonetheless, these types of measures are all traditional and proven tools of arms control. The next section explores the rich toolbox and spectrum of such measures.

CLASSICAL CONFIDENCE-BUILDING IN THE MILITARY AND NON-MILITARY DOMAINS

As noted earlier, the United Nations and the Organization for Security and Co-operation in Europe (OSCE) have a lot of experience in developing and promoting CBMs. Other regional organizations, such as the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF) and the Organization of American States (OAS), also discuss and consult on regional issues including the function and implementation of regional CBMs. The United Nations Disarmament Commission developed guidelines for CBMs, which were presented at a session of the General Assembly on 28 May 1988.[559] The major objective cited for the development of CBMs was "to reduce and even eliminate the causes of mistrust, fear, misunderstanding and miscalculations with regard to relevant military activities and intentions of other States". A central aim was "to help to prevent military confrontation as well as covert preparations for the commencement of a war, to reduce the risk of surprise attacks and of the outbreak of war by accident".[560]

Spurred during the Cold War because of the concern about nuclear war, the modern "arms control school" proposed and developed a number of different measures for crisis stability, damage limitation, and war prevention. A variety of arms control treaties and measures were introduced over time "to place political or legal constraints on the deployment and/or disposition

559 General Assembly, *Special Report of the Disarmament Commission to the General Assembly at its Third Special Session Devoted to Disarmament*, UN document A/S-15/3*, 28 May 1988, paras. 1.3–2.4.

560 Ibid., para. 2.2.6.

of national military means".[561] Confidence- and security-building measures (CSBMs) are an integral part of the arms control agenda.

During the early days of the Cold War, "nuclear confidence-building measures" were introduced as an initial step to increase transparency by the two military blocs. After the 1962 Cuban Missile Crisis, both superpowers established direct and effective communication hotlines to prevent the outbreak of a nuclear war caused by unauthorized or accidental use of nuclear weapons. In 1971, the superpowers signed the Agreement on Measures to Reduce the Risk of Outbreak of Nuclear War. In 1977, the Soviet Union and the United States broadened cooperation by signing the Agreement to Establish Nuclear Risk Reduction Centres, aimed at avoiding accidental nuclear war. Bilateral hotline agreements were also signed between the Soviet Union and France in 1976, and the Soviet Union and the United Kingdom in 1977.

After the end of the Cold War, proposals were made to reduce the high alert level of deployed, nuclear-equipped intercontinental ballistic missiles—de-alerting measures, that included removing the warheads from the missiles and storing them separately. In September 1998, US President Clinton and Russian President Yeltsin released a statement on the establishment of a Joint Data Exchange Center in Moscow for the exchange of information derived from each state's warning systems for the launch of ballistic missiles or space vehicles. Unfortunately, a Center was never realized, but risk reduction measures such as early warning were imperative in the nuclear standoff between the superpowers.

The most important multilateral nuclear agreement is the 1968 Treaty on the Non-Proliferation of Nuclear Weapons (NPT), which was extended indefinitely in 1995.[562] It aims to prevent the spread of nuclear weapons and weapons technology (articles 1–3), to promote cooperation in the peaceful use of nuclear energy (article 4), and to further the goal of achieving nuclear disarmament (article 6). An autonomous organization, the International Atomic Energy Agency (IAEA), helps to check compliance with the NPT, and has additional tasks in the area of nuclear safety,

561 S. Tulliu and T. Schmalberger, *Coming to Terms with Security: A Lexicon for Arms Control, Disarmament and Confidence-Building*, UNIDIR, 2003, p. 7.

562 The NPT was opened for signature in 1968, entered into force on 5 March 1970, and as of April 2013 had 189 states parties, including the five nuclear-weapon states. Four threshold nuclear-weapon states (the Democratic People's Republic of Korea, India, Pakistan, and Israel) are not members.

safeguards, and promoting the peaceful use of nuclear energy. Building confidence in the safe running of nuclear facilities and the non-diversion of nuclear material to underline peaceful use under article 4 is a key objective of the NPT regime.

An interesting regional approach has been the establishment in 1991 of the Brazilian–Argentine Agency for Accounting and Control of Nuclear Materials (ABACC), which was created after the rapprochement between both states after 1986. ABACC is a bilateral "safeguard agency" run by both states to guarantee that all nuclear material is exclusively used for peaceful purposes.

These agreements all include inspections, consultations, workshops, and concrete practical CSBMs and CBMs, which have helped to decrease mistrust between states, to reduce the dangers of armed conflict from misunderstandings and miscalculations in the nuclear weapons arena, and to build up additional insurance against an "outbreak" by a state.

Traditional arms control also can include bans on development, stockpiling, and use of certain types of weapons. The 1972 Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction (BTWC) prohibited the development, production, stockpiling, or acquisition of biological agents or toxins for non-peaceful purposes, as well as any related delivery means. The BTWC has no verification mechanism, but the states parties have agreed to use voluntary measures to declare high-security facilities or unusual outbreaks of diseases. The 1993 Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction (CWC) outlaws the production, stockpiling, retention, transfer, and use of chemical weapons and is administered by its own verification body, the Organization for the Prohibition of Chemical Weapons (OPCW).[563] Both conventions are restrictive in nature and are aimed at eliminating weapons based on dual-use substances—biological and chemical agents—that play an important role in daily life. Although specified lists of prohibited chemical or biological agents exist, both conventions also address future types of agents in a comprehensive way. The "general purpose criterion" that is enshrined in both conventions allows the development of a flexible list of prohibited agents. Complex technical and legal issues regarding

563 The CWC was signed on January 1993 and entered into force on 29 April 1997. It had 188 member states as of April 2013.

definitions, access to industrial facilities, verification of precursors, and so forth were successfully negotiated despite difficulties.

While arms control of nuclear, biological, and chemical weapons is mainly based on the control of precursor agents and materials, another approach is to restrict or regulate weapons delivery systems, such as missiles or aircraft. Missiles are the most ubiquitous delivery systems, but remain insufficiently restricted by arms control accords.[564] Supply-side arms export regulations, such as the 1987 Missile Technology Control Regime,[565] have helped to delay regional missile programmes and impede technological cooperation with non-member states. Many missile-related CBMs have been proposed, but never implemented universally.[566] One reasonably successful accord is the Hague Code of Conduct against Ballistic Missile Proliferation, which aims to enable more transparency concerning the spread of ballistic missiles. The politically binding Code was first signed on November 2002 and its signatories have increased to 134 states. Members have to provide pre-launch notification of ballistic missile and space launch vehicle launches and test flights, as well as to submit annual declarations of policy on ballistic missiles and space launch vehicles, including annual information on the number and generic class of ballistic missiles and space launch vehicles launched during the preceding year. Although the Code raised the level of awareness and transparency of the proliferation of ballistic missiles, key regions were left out, and cruise missiles, which can also carry weapons of mass destruction, are not covered by the agreement.

CONFIDENCE- AND SECURITY-BUILDING MEASURES

CSBMs are special military provisions and conflict-avoidance measures agreed by state parties "to dispel mistrust that otherwise lead to armed

564 Exceptions are the bilateral Strategic Arms Control Agreements between the Russian Federation and the United States, which also restrict the number of delivery systems.

565 The regime was established in 1987 by Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States. The number of partners has increased to a total of 34 states.

566 These include de-alerting, hotline agreements, notification of test flights, and visits to research and development facilities.

conflict".[567] They can be bilateral or multilateral, or can also be applied unilaterally, if one party implements CSBMs to induce another to act accordingly. In any case, CSBMs aim to influence the perception of others regarding one's intentions, as misperceptions about the capabilities and the national doctrines of a potential adversary can lead to armed conflict. "To dispel such mistrust, CSBMs seek to remove the inherent ambiguity surrounding national military policies by rendering these more transparent and by modifying these such that their potential for military aggression is demonstrably curtailed".[568] CSBMs can neither solve a conflict nor can they make war impossible, but they can increase trust, early warning, and predictability between states significantly. In the long run, they can modify, transform, and improve relationships between states, increase stability, and prepare the ground for robust arms control agreements. The Forum of Security Cooperation of the OSCE has been the primary forum for discussion and development of multilateral CSBMs.

Confidence- and security-building categories in Europe

In Europe, CBMs emerged after the 1975 Helsinki Conference on Security and Cooperation in Europe as a means to prevent a surprise attack or large-scale offensive operations in heavily militarized Central Europe. The Helsinki Final Act required the parties to give advanced notice of planned military manoeuvres involving more than 25,000 soldiers. In 1986, the Stockholm Agreement lowered the threshold for mandatory notification and made the invitation of observers from both superpower blocs obligatory. In 1990, the Vienna Document introduced a routine set of on-site inspections, based on annual exchange of information including on defence budgets and planning of new weapon systems, as well as establishing a regular dialogue between the NATO and Warsaw Pact militaries. After the end of the Cold War, the Vienna Document was revised and updated in 1992, 1994, 1999, and 2011. The Vienna Documents are directly connected to the 1990 Treaty on Conventional Armed Forces in Europe (CFE), which was signed on 19 November 1990, and came into force in November 1992. The CFE is seen as a major cornerstone for European security and a paradigm for cooperative

567 S. Tulliu and T. Schmalberger, *Coming to Terms with Security: A Lexicon for Arms Control, Disarmament and Confidence-Building*, UNIDIR, 2003, p. 135.
568 Ibid.

approaches to increase stability and security worldwide.[569] It marked the biggest wave of disarmament in the history of arms control and helped to transform the political architecture of Europe. Also related to the conventional arms control regime is the Treaty on Open Skies, which was signed in 1992 by NATO and the Warsaw Pact, and came into effect on 1 January 2002. Thirty-four member states agreed to conduct aerial inspection flights of each other's territory with airplanes equipped with certified sensors (photo, infrared) over extensive areas, spanning from the Atlantic to the Urals. The specially equipped airplanes with crews from other member states allow the cooperative observation of armed forces and military installations without relying on costly satellite technology. These procedures can also be used for the purpose of crisis management in specific conflict regions. The Open Skies Treaty is of unlimited duration and withdrawal requires six-months advance notification. It is in principle open for new states parties to join, and efforts were made to establish such a regional procedure for Latin America but failed to result in an accord.

Together with the Vienna Documents and the Open Skies Treaty, the CFE created a regime for transparency, dialogue, and cooperation on the basis of the OSCE framework. It implemented a stabilizing network of trust through notifications and inspections in the area between Vancouver and Vladivostok. Over 5,500 on-site inspections have been conducted among 30 CFE members establishing a transparent picture for Europe. A follow-on treaty, the Adapted CFE Treaty, was signed in Istanbul in 1999, but it was never ratified by the NATO states. The Russian Federation suspended the CFE in December 2007 and NATO followed suit by 2011, leaving the future of the conventional arms control regime in limbo. Despite—or perhaps because of—this loss, there is an ongoing need for CBMs related conventional armed forces in Europe.

Other regions also profited from the elaborated conventional arms control regime in Europe. The 1996 agreement on CSBMs in Bosnia and Herzegovina is modelled after the Vienna Documents. It imposes restrictions on the geographical deployment of armed forces and heavy equipment, and on the conduct of military exercises. It is part of the Dayton Agreement, the General Framework Agreement for Peace in

569 W. Zellner, H.-J. Schmidt, and G. Neuneck, *Die Zukunft der Konventionellen Rüstungskontrolle in Europa. The Future of Conventional Arms Control in Europe*, 2009, p. 15.

Bosnia and Herzegovina from 1995. A Joint Consultative Commission oversees implementation.

Confidence- and security-building categories outside Europe

Often the separation of military forces by demilitarized or thin-out zones has been introduced after bloody wars. After the October War in 1973 between Egypt and Israel, the Sinai Interim Agreement played an important part in the disengagement process. Demilitarized buffer zones flanked by thin-out zones were supervised by United Nations troops supported by aerial reconnaissance and early warning sensors. Later on, the Camp David Accords of September 1978 included thin-out zones and laid the foundation for the peace treaty between Egypt and Israel in 1979. In 1994, Israel and Egypt signed a peace agreement, in which both sides renounced threatening each other with armed forces and agreed to develop CSBMs. Talks between 1991 and 1995 to establish CSBMs in the Middle East—such as notification of certain military activities, avoidance of incidents at sea, maritime search and rescue coordination, military contacts, and the establishment of hotlines at the arms control and regional security talks—were ultimately suspended due to the tensions between Egypt and Israel over the nuclear weapons issue.

In Southern Asia, CSBMs have been used to alleviate military tensions at the borders between India and Pakistan, and China and India. In 1972, India and Pakistan pledged to refrain from the use of military force in Kashmir. In 1988, India and Pakistan concluded the Agreement on the Prohibition of Attack against Nuclear Facilities to prevent a surprise attack against each other's nuclear installations. In the 1990s, India and Pakistan concluded the Agreement on the Prevention of Aerospace Violations to secure each other's airspace as well as the Agreement for Advanced Notification of Military Exercises, Maneuvers and Troop Movements. After the Sino-Indian war in 1962, China and India introduced CSBMs by establishing a 20km demilitarized zone along the western part of the Himalayan border, the so-called Line of Actual Control. In the 1990s, agreements between China and India renewed commitments to restrict military deployments along the line of control.[570]

570 S. Tulliu and T. Schmalberger, *Coming to Terms with Security: A Lexicon for Arms Control, Disarmament and Confidence-Building*, UNIDIR, 2003, p. 141.

After the end of the Cold War, the Democratic People's Republic of Korea, the Republic of Korea, and the United States tried to develop CSBMs on the Korean peninsula. In 1991, the Agreement on Reconciliation, Nonaggression, and Exchange and Cooperation was signed, which included "the establishment of a joint reconciliation commission, as well as of a joint military commission charged with the elaboration of CSBMs including the limitation and advance notification of military exercises, the exchange of military information and personnel, and the installation of a hotline between national military commands".[571] Despite further efforts, such as the 1992 Joint Declaration on the Denuclearization of the Korean Peninsula and the 1994 Agreed Framework between the United States of America and the Democratic People's Republic of Korea, a peaceful solution for the nuclear programme of the Democratic People's Republic of Korea seems to be currently out of reach. It is important to note that while buffer zones or thin-out zones could increase the warning time of an attack, forces can be redeployed in a very short period of time.

Expert meetings and workshops were also held at the Conference on Disarmament in Geneva and within the OAS, which culminated in the 1995 Santiago Declaration that called on OAS members to implement a set of various CSBMs. This was expanded to the declaration of San Salvador in 1998, which included provisions such as political contacts and border cooperation, and cooperation on armed forces, military expenditures, and so forth.[572]

NON-MILITARY CBMS—A WIDER APPROACH

During the Cold War, CBMs were focused mainly on "hard" security issues (that is, they were CSBMs) to prevent violent outbreak of conflict in Europe and to reduce military tensions at the borders of the military blocs. The 1975 Helsinki Final Act also included a set of non-military CBMs. For non-military CBMs there is no commonly accepted definition, but the OSCE Guide on Non-military Confidence-Building Measures, which was developed by the OSCE's Center for Conflict Prevention, works with the following definition:

> Non-military confidence building measures are actions or processes undertaken in all phases of the conflict cycle and

571 Ibid., pp. 155–156.
572 Ibid. pp. 138–139.

> across the three dimensions of security in political, economic, environmental, social or cultural fields with the aim of increasing transparency and the level of trust and confidence between two or more conflicting parties to prevent inter-State and/or intra-State conflicts from emerging, or (re-) escalating and to pave the way for lasting settlement.[573]

CBMs can become important in intrastate conflicts, in which police and security forces are confronted with violent opponents or paramilitary troops. The OSCE has experience in regions with intrastate conflicts that have military, economic, and cultural dimensions. Civil confidence-building measures (CCBMs) are designed to build trust and confidence among civil communities such as ethnic groups or local governments which represent minority groups.[574] Transparent discussions or decision-making processes with the participation of conflict parties can help to reduce fears and feelings of insecurity among ethnic groups. CCBMs can build bridges to CSBMs. For example, CCBMs can help in post-conflict situations where communication between conflicting parties is broken down or complicated. Discussions of CCBMs can bring responsible people and representatives together and help lay the groundwork for CSBMs.

Some of the traditional CSBM techniques can also be useful for CCBMs. For example, the establishment of hotlines for direct exchange of information between police or non-military forces can help to strengthen confidence in state entities and foster cooperation.

TRANSPARENCY AND CONFIDENCE-BUILDING FOR CYBER AND OUTER SPACE ACTIVITIES

Cyberspace is dominated by dual-use technologies that can have military as well as commercial and civilian applications. It is also a technical domain in which private sector actors control most of the assets. In both these ways, cyberspace is quite similar to the space domain. Missile and rocket technologies are vectors for military payloads such as nuclear weapons, but can also serve as space launch vehicles for civil or commercial payloads. Outer space, like cyberspace, is an important strategic asset for national

573 OSCE Conflict Prevention Centre, *OSCE Guide on Non-Military Confidence Building Measures (CBMs)*, 2012, p. 9.

574 S. Tulliu and T. Schmalberger, *Coming to Terms with Security: A Lexicon for Arms Control, Disarmament and Confidence-Building*, UNIDIR, 2003, p. 157.

and international security—despite its highly commercial infrastructure. Thus, there is some value in reviewing the specific TCBMs that have been proposed for outer space with an eye to future solutions for cyberspace.

The overarching international framework for outer space, including the concepts of "peaceful use" and "free access", are codified in the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, known as the Outer Space Treaty (OST). Although the deployment of weapons of mass destruction in orbit is prohibited under article 4 of the OST, the deployment and use of conventional space weapons is not excluded explicitly. Over the decades since the OST, a number of initiatives have been launched by states and non-governmental organizations to prevent the weaponization of space and to keep the space environment free from potential armed conflict—including the 2008 proposal by China and the Russian Federation for the Conference on Disarmament to negotiate a treaty to ban weapons placed in space, the Draft Treaty on the Prevention of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects. The Conference on Disarmament has not succeeded, however, to negotiate any multilateral agreement regarding military space activities since it began work on the subject in the mid-1990s.

Indeed, as most efforts to develop bilateral or multilateral space arms control measures have come to naught, recent efforts to protect the space domain have centred on the development of CBMs and norms of conduct.

In December 2008, the European Union published the Draft Code of Conduct for Outer Space Activities, subsequently revised in 2010. This effort is aimed at establishing non-legally binding norms of behaviour in space. The proposed international code is intended to enhance "the safety, security and predictability of outer space", and includes both civilian and military provisions. For example, the proposal seeks to minimize "the possibility of accidents in space, collisions between space objects or any form of harmful interference" (article 4.1).

The United Nations began studying the question of TCBMs for outer space in 1991. A General Assembly resolution in 2006, spearheaded by the Russian Federation, asked United Nations Member States for concrete proposals on such measures; the Russian Federation in 2009 put forward a detailed set of potential measures that ranged from basic transparency

measures to "rules of the road" for space activities.[575] In 2010, the General Assembly mandated a Group of Governmental Experts to explore TCBMs; the group began its work in July 2012 and will wrap up in July 2013. The goal is to reach agreement on a series of recommendations for TCBMs to the Secretary-General. Concepts widely discussed have included the notification of launches, orbital changes, and high-risk re-entries of satellites into the atmosphere. In addition, the United Nations Committee for the Peaceful Uses of Outer Space (COPUOS), comprising 69 Member States, is studying new multilateral, voluntary measures for ensuring "the long-term sustainability" of the space environment. While this effort is highly technical and focused on "best practice guidelines", many of the measures required for ensuring safe and secure space operations, such as exchange of data regarding objects on orbit, are also functional TCBMs. This work is expected to be completed in 2014.[576]

575 Permanent Mission of the Russian Federation to the United Nations Office and other International Organizations in Geneva, "Transparency and confidence-building measures in outer space activities and the prevention of placement of weapons in outer Space", www.geneva.mid.ru/disarm/d-01.html.

576 Committee on the Peaceful Uses of Outer Space, *Draft Report of the Working Group on the Long-Term Sustainability of Outer Space Activities*, UN document A/AC/105/C.1/LTS/2012/L.1, 16 February 2012.

CHAPTER 3

TOWARDS TCBMS IN THE CYBERSPHERE

Götz Neuneck

When developing and introducing TCBMs for the cybersphere, it is necessary to deal with key challenges and questions complicating the process. First, confidence *where*, that is, what is the cybersphere? Second, confidence about *what*, that is, what is the concern? And third, confidence for *whom*, that is, who are the actors that need to feel confident? Numerous problems in defining terminology thus far have not been dealt with in a sufficient manner. In particular, it is essential for the international community to find a common language for key terms such as cyberwar, cyberattack, cyber tools and cyberweapons, cyberdefence and offence, and so forth, to form a basis for future dialogue and cooperation. Finding common language in itself would be a CBM.

Cyberspace is notoriously difficult to describe and to define due to the breathtaking speed of technological innovation and the rapid increase in users and types of use. The Cyber Security Strategy of the United Kingdom describes cyberspace 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".[577] Cyberspace is not like the geographical domains land, air, sea or outer space—it is instead a totally artificial domain.

The "cyber domain" is built on globally connected networks of hardware with common processing architectures that allow the exchange of packetized data.[578] Computers use standardized protocols to communicate with each other using the full electromagnetic spectrum via undersea cables, satellite links, fibre optics, and microwave links. Cyberspace should not be confused with the Internet, which is only a part of it. Many "end user" technologies and hybrids, such as telephones, televisions, or

577 United Kingdom, *The UK Cybersecurity Strategy: Protecting and Promoting the UK in a Digital World*, 2011.

578 B. Weeden, "Cyber offence and defence as mutually exclusive national policy priorities", *Disarmament Forum*, no. 4, 2011, p. 19.

cameras are also connected in cyberspace and their numbers are growing exponentially. The swift life and innovation cycles of hardware and software and the demands of the market create all kinds of vulnerabilities. Closing these gaps by hardening hardware and software to defend national assets means to strengthen "cybersecurity." While cyberdefence (such as firewalls) is seen as a necessary and there is much legal activity to mitigate cyberattack at all levels of cyberspace, some states already regard the offensive use of cyber tools for prevention and deterrence as a legitimate option. This, in turn, has led to the ongoing debate about applying the laws of armed conflict, especially the "inherent right of self-defense" under Article 51 of the Charter of the United Nations, and also to uncertainty about what constitutes a "strategic cyberattack", which crosses the line of an "armed attack" and that again would trigger certain legal determinations.[579] In the case of a severe cyberincident, a clear identification of the aggressor, the potential damage, and the originating location of the attack must be determined with high confidence. As noted earlier, in this regard, the characteristics of cyberspace complicate the situation. In particular, attribution is hard to achieve, because the connection between an attacker and a specific cyber action is very difficult to prove. Offensive actions can be conducted with great rapidity, and the true extent of any damage might only be identified well after the attack. Disruptive cyber tools are widely available, legally and illegally, and can be used as a relatively inexpensive method of covering the identity of the perpetrator. James Lewis concluded: "Cyber attack is a behavior rather than a technology".[580]

A United Nations Group of Governmental Experts stated in a 2010 report that cyberspace has become "an arena for 'disruptive activity'" and that cyber threats are becoming "the most serious challenges of the 21st century".[581] Five General Assembly resolutions underlined the national responsibility to introduce defensive measures as a domestic effort. It is of utmost importance that governments and the private sector coordinate their activities to strengthen national cybersecurity and develop trusted

579 N. Melzer, "Cyber Operations and *jus in bello*", *Disarmament Forum*, no. 4, 2011.

580 J.A. Lewis, "Confidence-building and international agreement in cybersecurity", *Disarmament Forum*, no. 4, 2011, p. 58.

581 General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/65/201, 30 July 2010, p. 2.

methods of information security. Additionally, creating resilient critical infrastructures and effective law enforcement is obligatory. Countries that have neither the expertise nor the skilled personnel have to be supported by briefings, workshops, and joint training. Reports in 2010 and 2011 by the United Nations Secretary-General to the General Assembly focused on "developments in the field of information in the context of international security".[582] Longer statements by Australia, Germany, the Netherlands, and the United States to the General Assembly include proposals for principles, rules, and norms for behaviour, and some concrete recommendations. The following general "principles" have been proposed as important elements for secure management of the global commons of the Internet: availability, confidentiality, competitiveness, integrity, authenticity of data and networks, privacy, and protection of intellectual property rights.[583] Other "responsibility rules for states" such a territoriality, cooperation, self-defence, data-exchange, early warning, and so forth, have been recommended as a starting point for discussions. These principles could also be the vantage point for future CBMs in cyberspace.

Treaty-based arms control models such as a "cyberweapon convention" further have been proposed to secure cyberspace and to prevent further proliferation of new cyberweapons. Preventive arms control agreements, such as the OST, the BTWC, the CWC, and the Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (the Environmental Modification Convention), ban whole classes of threats and weapons; indeed the CWC in particular has been proposed as a model for cyber arms control.[584]

Regulatory-oriented arms control treaties, such as the Strategic Arms Reduction treaties or the CFE, limit certain weapon systems geographically or operationally. Arms control agreements can cover the whole "arms life cycle", starting from research and development, to stockpiling and deployment, to dismantlement. Such treaties can also limit the acquisition

582 General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/65/154, 20 July 2010; and General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/66/152, 15 July 2011.

583 See E. Tikk, "Ten rules for cyber security", *Survival: Global Politics and Strategy*, vol. 53, no. 3, 2011.

584 K. Geers, *Strategic Cyber Security*, NATO Cooperative Cyber Defense Centre of Excellence, 2011, pp. 123–131.

of weapons in an early stage of the development. However, given the dual-use nature of cyber technology and the realm itself, a prohibition on research and development of cyberweapons would be nearly impossible to verify and it is therefore infeasible.[585]

Another approach is the normative approach, such as a restriction upon the first use of cyberweapons. David Eliot argues that some arms control treaties, such as the Environmental Modification Convention, which aims to ban military or other hostile uses of environmental modification techniques, prohibits first use. A number of states have used declaratory "no first use" statements in other domains, but it is often pointed out that such declarations are easily reversible and, of course, cannot guarantee that other potential aggressors are not preparing themselves for such an attack. James Lewis argues that in the cyber domain a no-first-use commitment also requires states to renounce cyberespionage, because the techniques of attack and espionage are similar.[586] This latter point could be a big obstacle to any no-first-use agreement, as many states already are engaged in cyber espionage.

The "general use" (as well as the possession, stockpiling, and transfer) of biological and chemical weapons is clearly prohibited by the BTWC and CWC. However, it is again hard to fathom how this could be applied in the cyber domain, given the lack of clarity about what constitutes a weapon and the basic fact that most cybertechnologies have multiple uses.

Some states already have declared that the norms and obligations of the law of armed conflict can be applied to the use of cyberweapons.[587] But to implement appropriate measures in the cyber realm based on the principles of proportionality, distinction, and discrimination is not an easy task. That said, agreements could be made based on a list of facilities, such as hospitals or water supplies, that are not allowed to be attacked kinetically or electronically. It has also been proposed for states "to take measures to electronically identify systems as being associated with prohibited targets". Exercises and training courses with computer specialists, the military, and legal advisors could help to overcome

585 See H. Lin, "Some modest steps toward greater cybersecurity", *Bulletin of the Atomic Scientists*, vol. 68, no. 5, 2012.

586 J.A. Lewis, "Confidence-building and international agreement in cybersecurity", *Disarmament Forum*, no. 4, 2011, p. 57.

587 See N. Melzer, "Cyber Operations and *jus in bello*", *Disarmament Forum*, no. 4, 2011.

misperceptions and establish procedural clarity. Discussions could be arranged to explore extending prohibited targeting lists to include other national critical infrastructure, such as electrical power networks, financial systems, or telecommunications. In addition, cyberattacks could be prohibited against certain types of multilateral activities such as United Nations peacekeeping operations, international maritime activities, and transport for disaster relief.

Several practical transparency measures could be established in peacetime to reassure states that efforts in cyberdefence are not preparations for attack. For example, a "cyber doctrine seminar" at the OSCE level could be an important step forward, based on the positive experiences of the military doctrine seminar series already held by OSCE states. Key discussion items could be the exchange of national cyber strategies, and of the scope, decision-making, administrative structures, and institutional settings responsible for cyberdefence. Points of contact and best practices shared through cyber exercises could also be established. Actors from civil society and the private sector should be invited to offer their expertise; observers from other countries and regional organizations such as the ARF and OAS could be invited as well. An equivalent seminar about national civilian cybersecurity strategies could be organized at the United Nations level.

Such a forum also could be used to agree upon stability and risk-reduction measures, for example, establishment of communication links to exchange information about cyberincidents and development of a process for notification of cyber-related military exercises. Special risk reduction centres at the national level could be set up for handling such information exchanges. Practical cooperation in the field of cyber forensics and cyber non-proliferation would help to build trust. To further bolster such cooperation, governments could make written commitments in their cyber strategies regarding acceptance of legal responsibility to help to identify cyberattackers working from their territory.

Finally, cooperation among those states with robust cyberdefences to help build capacity in others could also serve to build confidence all around. Not all states have the resources, skills, and expert knowledge to set up national cyberdefence institutions. Joint workshops and exercises could be established at the regional level, for example.

CONCLUSION

It is clear that the issue of cybersecurity, and how international and regional security may be impacted by cyber activities, is coming to the forefront of multilateral debate. However, it is also clear that there remain among states competing threat assessments and concepts for potential responses. There is lack of agreement about the role multilateral bodies and instruments should play. Further, the technical communities and the political/military communities remain blocked in an unhelpful way, given the complex, inter-related problems facing the cybersphere. At the same time, the international community is beginning to grasp that securing the cybersphere and preventing conflict, either in the cyber domain or sparked by cyberattacks, will require multilateral approaches.

The overall goal of developing and implementing future norms, rules, and regulations, such as international guidelines or principles of appropriate state behaviour, is to maintain and further develop a peaceful, safe, stable, and predictable cyberspace. This will require more focused multilateral cooperation and a multi-stakeholder process. The debate is at an early stage; much work remains to be done.

ABBREVIATIONS

APCERT	Asia Pacific Computer Emergency Response Team
ARF	ASEAN Regional Forum
ASEAN	Association of Southeast Asian Nations
BTWC	Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction
CBM	confidence-building measure
CCBM	civil confidence-building measure
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CERT	computer emergency response team
CFE	Treaty on Conventional Armed Forces in Europe
CFSP	European Common Foreign and Security Policy
CICTE	OAS Inter-American Committee Against Terrorism
CIRT	computer incident response team
CSBM	confidence- and security-building measure
CSIRT	computer security incident response team
CWC	Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction
GGE	group of governmental experts
IAEA	International Atomic Energy Agency
ICT	information and communications technology
ITU	International Telecommunication Union
NATO	North Atlantic Treaty Organization
NPT	Treaty on the Non-Proliferation of Nuclear Weapons
OAS	Organization of American States

OECD	Organisation for Economic Co-operation and Development
OPCW	Organisation for the Prohibition of Chemical Weapons
OSCE	Organization for Security and Co-operation in Europe
OST	Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies
SCO	Shanghai Cooperation Organization
TCBM	transparency and confidence-building measure