UNIDIR RESOURCES

# Cybersecurity and Cyberwarfare
2011

## Cybersecurity and Cyberwarfare

Preliminary Assessment of National Doctrine and Organization

Center for Strategic and International Studies

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 of boundaries.

***

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

***

## About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, non-profit organization headquartered in Washington, D.C. CSIS conducts research and analysis and develops policy initiatives that anticipate change. More than 220 full-time staff and a large network of affiliated scholars focus their expertise on defence and security, on the world's regions and their unique challenges, and on the issues of an increasingly connected world. CSIS does not take specific policy positions; accordingly, all views expressed in this publication should be understood to be solely those of the authors.


## Authors

James A. Lewis, Katrina Timlin

## Research Assistants

Steven Deitz, Allison Kempf, Jarrod Rifkind, Joshua McGee, Alex Lukich

# Cybersecurity and Cyberwarfare

## Preliminary Assessment of National Doctrine and Organization

With the development of the internet as a global infrastructure for business and as a new tool for politics, espionage and military activities, cybersecurity has become central topic for national and international security. The states addressed in this preliminary assessment were selected by looking at their levels of military spending and the degree of internet connectivity, assuming that those states with low military spending and little internet connectivity would be less likely to have cyber capabilities (we also did a random sample of the states in this less-connected category to test this assumption).

Using open-source literature, we reviewed policies and organizations in 133 states to determine how they are organized to deal with cybersecurity, whether they have a military command or doctrine for cyber activities, and whether they have or plan to acquire offensive cyber capabilities. There are clear limitations to open-source data. Many states are secretive about the nature of their planning and capabilities for cyberwarfare, although most are more open about their law enforcement and domestic security arrangements for cybersecurity. Despite this, we were able to find general information on the development of new military cyber capabilities.

We identified 33 states (detailed in section I) that include cyberwarfare in their military planning and organization. These range from states with very advanced statements of doctrine and military organizations employing hundreds or thousands of individuals to more basic arrangements that incorporate cyberattack and cyberwarfare into existing capabilities for electronic warfare. Common elements in military doctrine include the use of cyber capabilities for reconnaissance, information operations, the disruption of critical networks and services, for “cyberattacks”, and as a complement to electronic warfare and information operations. Some states include specific plans for informational and political operations. Others link cyberwarfare capabilities with existing electronic warfare planning. The linkages between electronic warfare and cyberwarfare are likely to be an area of expanded attention as computer networks (or their access points) become increasingly mobile and wireless.

We also discuss another 36 states (detailed in Section II) where there is no public discussion of a military role in cyberspace and where civilian agencies charged with internal security missions, computer security or law enforcement are responsible for cybersecurity. This is, in some ways, the “traditional” approach to cybersecurity that dates back to the 1990s—setting up a national Computer Emergency Response Team (CERT), assigning responsibility to science ministries and creating specialized units within the national police. It would not, however, be difficult for these states, if they wished, to translate their defensive and civilian capabilities into military cyber capabilities. Knowledge of cyberdefence can inform offensive operations and the skills needed to defend a network can also be used to attack.

The cutting edge for military organizations is the creation of specific commands dedicated to cyberwarfare. The alternative is to embed cyber capabilities in existing military organizations for electronic warfare, in general staffs or intelligence organizations. Cybercommands can be seen as an organizational experiment. The most salient example

is, of course, the United States, which announced the creation of a cybercommand in 2009. This very public announcement served as a model for other states. Like the US cybercommand, most of these organizations have defensive and offensive missions: to secure national networks and to prepare offensive capabilities. Public information is available on 12 states that have established or plan to establish within the next year military cyberwarfare organizations—Argentina, Brazil, Canada, China, the Democratic People's Republic of Korea, Denmark, Germany, India, Iran, the Republic of Korea, Switzerland and the United States. It is likely, however, that other states, such as Cuba or the Russia Federation, are also developing such organizations; unfortunately, public information on these activities is not available.

Even with the limitations on available data, this preliminary assessment suggests that cyberwarfare has become an unavoidable element in any discussion of international security. Cyber capabilities are attractive as a cost-effective asymmetric weapon. Informational advantage and networks attack play a large role in modern strategy. Defending computer networks is a concern for many states. Most major military powers have developed cyberwarfare capabilities and doctrine and more states will acquire these capabilities in the future. Airplanes were once possessed by only a few states and had limited military value, but then grew into a key component of military power possessed by most states. Military cyber capabilities appear to be on the same path. This trend raises questions regarding norms for cyberwarfare, the obligations of states regarding the application of offensive cyber capabilities, and the applicability of existing laws of war and norms on use of force in cyberspace.

# States with Military Doctrine and Organizations for Cybersecurity and Cyberwarfare

## Albania

In 2010, the Albanian Ministry of Defence created the Interinstitutional Maritime Operational Center (IMOC).[1] The Center's responsibilities include civil emergencies, airspace control, and developing cyberdefence capability.[2] Albania views cyberattacks as an emerging threat but does not yet have a national cyber strategy. Albania is working with the United States to improve its cybersecurity capabilities. On 13 June 2011, the United States Agency for International Development launched the Albanian Cyber-Security Program, a one-year initiative to improve Albania's ability to prevent and respond to cybersecurity incidents.[3]

## 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 one's own networks and offensive measures to disrupt those of the enemy.[4] The task of developing joint military doctrine for communications and electronic warfare falls to Jefatura VI (responsible for command, control, communications, information technology and interoperability) of the armed forces.[5] 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.[6]

## Austria

The Austrian Ministry of Defence cited cybersecurity as a major component of Austria's defence strategy in its 2008 *White Book*, and cybersecurity is considered a priority. The *White Book* included plans to restructure the cabinet offices in 2009 to include a cyber component.[7] Austria's recent national security strategy, *Shaping Security in a New Decade*, was released in March 2011. It addresses contemporary threats, including

1 "The first annual analysis of the Interinstitutional Maritime Operations Center was held", Albanian Ministry of Defence, 21 December 2010.

2 "Defence Minister, Mr. Arben Imami Assesses the Work of MOD and AFs for 2010 and Sets Targets for 2011", Albanian Ministry of Defence, 20 January 2011; *National Strategy on Integrated Border Management and its Action Plan*, Albanian Ministry of Interior, Ministry of Finance, Ministry of Agriculture, 2006.

3 "USAID launches the Albanian cyber-security program", United States Agency for International Development, 13 June 2011.

4 Javier Ulises Ortiz,"Argentina: The Challenge of Information Operations", *IOSphere*, 2008, <www.au.af.mil/info-ops/iosphere/08special/iosphere_special08_ortiz.pdf>, pp. 61–62.

5 "Organizacion Del Estado Mayor Conjunto", <www.fuerzas-armadas.mil.ar/institucional/organigrama.asp>.

6 Javier Ulises Ortiz, "Argentina: The Challenge of Information Operations", *IOSphere*, 2008, <www.au.af.mil/info-ops/iosphere/08special/iosphere_special08_ortiz.pdf>, p. 60.

7 *Weissbuch 2008*, Bundesminister fuer Landesverteidigung und Sport, 2009, <www.bmlv.gv.at/pdf_pool/publikationen/weissbuch_2008.pdf>, pp. 15, 85.

cybersecurity.[8] The Abwehramt, a military intelligence organization in Austria, cites electronic defence, including malware protection, as one of its core responsibilities.[9]

## Australia

The Australian Cyber Security Strategy, released in 2009, seeks to enable a secure operating environment for both government and private networks in order to ensure security and to take advantage of the economic benefits of information technology. Australia identified seven strategic priorities: developing threat awareness and response, changing civilian security culture, promoting public–private partnerships, securing government systems, pursing international engagement, creating an effective legal framework and building a skilled cyber workforce.[10] Cybersecurity policy is coordinated by the Cyber Security Policy and Coordination Branch of the Attorney-General's Department.

The Cyber Security Operations Centre was established in 2009 as mandated by the strategy.[11] 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.[12] The primary 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.[13]

The Defence Science and Technology Organisation announced in 2008 that it would "increase its investigation and application of key enabling technologies which will provide significant returns for development of the future force, such as ... cyber warfare (including computer security)".[14] The Organisation has an annual budget of approximately $440 million and a staff of around 2,600.[15] The Australian Security Intelligence Organization established a cyber-investigations unit in March 2011. It will focus on response and intelligence regarding "state-sponsored cyberattack".[16] The unit operates under the supervision of the First Assistant Director-General for Counter-Espionage and Interference.[17]

## Belarus

Belarusian military doctrine refers to cyberconflict or cyberwarfare as "information confrontation". According to national doctrine, one of the main external threats facing the state is the potential for informational influence used to the disadvantage of Belarus or

8 Georg Mader, "Austria Unveils New Security Doctrine Amid Neutrality Concerns", *Jane's Defence Weekly*, 8 March 2011.

9 Benjamin S. Buckland, Fred Schreier and Theodor H. Winkler, "Democratic Governance and the Challenges of Cyber Security", DCAF Horizon 2151 Working Paper 1, Geneva Centre for the Democratic Control of Armed Forces,. <http://genevasecurityforum.org/files/DCAF-GSF-cyber-Paper.pdf>, p. 33.

10 Attorney-General's Department, *Cyber Security Strategy*, Australia, 2009, p. vii.

11 Ibid.

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

13 Attorney-General's Department, *Cyber Security Strategy*, Australia, 2009, p. vii.

14 Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030*, Australia, 2009, p. 134.

15 "About DSTO", Defence Science and Technology Organisation, <www.dsto.defence.gov.au/page/76/>.

16 Tom Espiner, "UK helps Australia's cyber-spy unit get to work", *ZDNet UK*, 11 March 2011.

17 See ASIO Senior Management Organization Chart, <www.asio.gov.au/img/files/Unclassified-Org-Chart.pdf>.

its allies. The Belarusian approach to cyberdefence is two-fold—the military is developing cyber capabilities to provide early warning of a cyberattack.[18]

In peacetime, the Belarus Armed Forces are responsible for ensuring informational security, and in wartime, as part of their "offense repulsion" capability, they are trained in informational confrontation and counteraction against enemy forces.[19] In 2001, Belarus signed an agreement on cooperation with the Commonwealth of Independent States, which contains a provision on assistance in the event of a cyber incident.[20]

## Brazil

Brazil's 2008 *National Strategy of Defense* established the guidelines for reorganizing the Armed Forces and for adapting the defence industry to ensure domestic provision of needed technologies for the navy, army and air force. Along with space and nuclear technologies, it identifies "cybernetics" as a strategic sector for national defence.[21]

Brazil has established a Cyber-Warfare Communication Centre, led by a Brigadier General, in response to numerous probes of Brazilian military networks.[22] Brazil's defence strategy stresses the importance of indigenous cyber capacities and technological self-sufficiency. Cyber technologies considered particularly important are those used in submarines and weapons systems. Maintaining indigenous cyber capabilities will involve building cyber capacity in educational institutions and in the military to enhance communication among components of the armed forces. The Strategy calls for the establishment of an organization dedicated to enhancing cyber capabilities in industry and the military.[23] To contribute to regional stability and cybersecurity, the Ministry of Defense will strengthen strategic partnerships with friendly states in the region and in the Community of Portuguese Language Countries.[24]

In 2010, Brazil and the United States signed a Defense Cooperation Agreement. Areas of cooperation include research and development, joint military exercises, and student exchanges and education cooperation. Military exercises include cybersecurity, as Brazilian personnel have participated in US Department of Defense-sponsored workshops and virtual exercises on cyberdefence.[25]

Brazil's International Security Office announced the creation of the Center of Cyber Defense, based in Brasilia, to protect critical military, governmental and information infrastructure. The Center will be staffed by 100 officials from the army, air force and navy. The Center is expected to become operational by the second half of 2011. Currently,

18 The Military Doctrine of the Republic of Belarus, <www.mod.mil.by/doktrina_eng.html>, chp. 2, §§ 7, 10.

19 Ibid., § 7.

20 Vladimir Golubev, "Fighting cybercrime in CIS: strategies and tactics", Computer Crime Research Center, <www.crime-research.org/articles/golubev_Jul/>.

21 The Strategy does not define cybernetics, and the term is subject to various interpretations depending on context. For the purposes of this study, we assume cybernetics to mean the communication within and the control of networked systems; *National Strategy of Defense*, Brazilian Ministry of Defense, 2008.

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

23 *National Strategy of Defense*, Brazilian Ministry of Defense, 2008, pp. 33–34.

24 Ibid., p. 64.

25 "U.S.–Brazil Defense Cooperation Agreement (DCA)", US Department of State, 12 April 2010.

the International Security Office is responsible for the security of public administration networks.[26]

## Canada

Canada's *Cyber Security Strategy* was issued in October 2010.[27] The Strategy focuses on securing both government and critical infrastructure networks, as well as educating the Canadian public about cyber threats. Public Safety Canada, the government agency responsible for public safety and emergency preparedness, will oversee the implementation of the Strategy.[28] The Strategy also addresses international engagement between the Department of National Defence and allied militaries on cyberdefence best practices.[29] The Canadian Security Intelligence Service lists information security threats as one of its five priority areas.[30]

The Canadian army has an electronic warfare centre and a network operation centre, both of which support military cyber capabilities. The Canadian Forces Network Operation Centre is under the Command of the Canadian Forces Information Operations Group, and its mission is to "gain and maintain cyber superiority".[31]

## China

In early 2000, China's Central Military Commission (called for a study of people's war under conditions of "informationalization". China's 2004 *White Paper on National Defence* stated that "informationalization has become the key factor in enhancing the warfighting capability of the armed forces" and that the People's Liberation Army (PLA) takes informationalization "as its orientation and strategic focus". Chinese military doctrine advocates a combination of cyber and electronic warfare capabilities in the early stages of conflict.[32]

While the White Paper identifies the PLA Air Force as responsible for information operations and information counter-measures, outside observers believe that the PLA General Staff Department's 4th Department, which oversees electronic counter-measures and research institutes developing information warfare technologies, is responsible for military cyber capabilities. The 3rd Department is responsible for signals intelligence and focuses on collection, analysis and exploitation of electronic information.[33] The 4th and 3rd Departments conduct advanced research on information security.[34] The PLA also

26 Hadley Richardson, "Brazil raises cyber defense game," *[it]decisions*, 15 June 2011.

27 *Canada's Cyber Security Strategy*, Public Safety Canada, 2010.

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

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

30 *Our Priority Areas,* Canadian Security Intelligence Service, 3 August 2011, <www.csis-scrs.gc.ca/prrts/index-eng.asp>.

31 "Canadian Forces Network Operations Center", National Defence and the Canadian Forces, <www.img.forces.gc.ca/org/cfi-goi/cfnoc-corfc-eng.asp>.

32 "China's National Defense in 2004", Information Office of the State Council of the People's Republic of China, 2004, <http://english.peopledaily.com.cn/whitepaper/defense2004/defense2004.html>.

33 Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation", Northrop Grumman Corporation, prepared for the US–China Economic and Security Review Commission of the United States Congress, 2009, <www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf>, pp. 6, 31.

34 Ibid, pp. 30, 32.

maintains ties with research universities and the public sector to improve its capabilities, with some units directly embedded in commercial firms and universities.[35]

## Colombia

The Colombian Ministry of Foreign Relations established an interagency 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 Foreign Ministry and the Ministry of the Interior and Justice assigned cybersecurity responsibilities to the Ministry of Defence. Colombia created a national CERT in 2009.[36] The Ministry of Defence is the lead agency implementing and operating the CERT, although legislative, judicial and international matters are handled by the respective agencies. The CERT is one aspect of a national cybersecurity policy that coordinates the public and private sectors in strengthening future defences.[37]

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.[38]

## The Democratic People's Republic of Korea

The Democratic People's Republic of Korea is believed to invest significant resources in its offensive cyber capabilities, but there is little official information on its activities. External sources speculate on the creation of specialized units in the military. Several universities have been identified as being involved in training and offensive operations.[39]

## Denmark

Danish military doctrine references cyberspace as a military battle space but does not provide details of concrete technical and operational capacity. Danish cyber strategy is defensive and focused on protecting military computer systems from exploitation or disruption, without an explicit focus on developing offensive or response mechanisms.[40]

35 Ibid, p. 33.

36 "Ciberseguridad y Ciberdefensa: Una Primera Aproximacion", Colombian Ministry of National Defence, 2009.

37 See <www.cert.org.co>.

38 "Ciberseguridad y Ciberdefensa: Una Primera Aproximacion", Colombian Ministry of National Defence, 2009.

39 Two universities allegedly involved in cyberwar research are Mirim College and Moranbon University; Lee Seok Young and Kwon Eun Kyoung, "A look at Mirim College, hotbed of cyber warfare", *Daily NK*, 6 May 2011; Jung Kwon Ho, "Mecca for North Korean hackers", *Daily NK*, 13July 2009.

40 *Danish Defence Agreement 2010–2014*, 24 June 2009, p. 11.

The Danish Defence Agreement 2010–2014 calls for the establishment of a cyber network operations unit.[41] The Defence Intelligence Service is responsible for finding and preventing cyber threats and is planning to build a cyberwarfare unit.[42] The Danish Defence Commission has recommended establishing computer networking operations in order to promote Denmark's cyber capabilities and to protect the information technology of the armed forces from cyberattack.[43] The Danish army also has the 3rd Electronic Warfare Company (a part of the Telegrafregimentet, a support regiment created in 1951), whose purpose is to disrupt or exploit enemy communications.[44]

Denmark will also participate in the "Nordic Resource Network", which seeks to improve cyberdefences.[45]

## Estonia

The 2007 Estonian cyber incident catalyzed the state's development of cyber capabilities and policies. The Ministry of Defence coordinates the state's cyberdefences.[46] The Defence League, a voluntary national defence organization, is organized and trained by the Ministry of Defence and is currently developing its cyberdefence capabilities.[47] The cyber unit within the Defence League, the Cyber Security Alliance, has three main tasks: protection of the Estonian "e-lifestyle", training IT specialists and sharing information on cybersecurity with the public.[48]

A national cybersecurity strategy was drafted by the Cyber Security Strategy Committee, formed after the 2007 incident. 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. A Cyber Security Council was established in the Security Committee of the Government of the Republic to implement this strategy.[49] The goal of the strategy is to decrease Estonian vulnerability in cyberspace, prevent cyberattacks and restore critical infrastructure as quickly as possible in the event of such an attack. To this end, the strategy identifies the following strategic goals: establishing a multilevel system of security measures, expanding expertise in information security, instituting regulatory reforms and fostering international cooperation. A unit within the Ministry of Economic Affairs would ensure the security of state information systems.[50]

41 Ibid, pp. 11, 28.

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

43 *Danish Defence Agreement 2010–2014*, 24 June 2009, p. 11.

44 "Electronic Warfare Kompagni", <www.forsvaret.dk/TGR/Organisation/3%20EWKMP/Pages/default.aspx>.

45 "Denmark Country Report", European Network and Information Security Agency, <www.enisa.europa.eu/act/sr/files/country-reports/Denmark.pdf>, 2011, p. 16

46 Estonian Ministry of Defence, *Cyber Security Strategy*, 2008, <www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf>.

47 Henry Kenyon, "Volunteer cyber corps to defend Estonia in wartime", *Defense Systems*, 12 January 2011, <http://defensesystems.com/articles/2011/01/12/estonia-cyber-defense-league-army.aspx>.

48 "Federal Cyber Security", Estonian National Defense League, <www.kaitseliit.ee/index.php?op=body&cat_id=395>.

49 *Cyber Security Strategy*, Estonian Cyber Security Strategy Committee, 2008, <www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf>, pp. 8, 29.

50 Ibid, pp. 27, 29.

Estonia places significant emphasis on its NATO membership and international cooperation as a means to augment its defence capabilities. The NATO Cooperative Cyber Defence Centre of Excellence, established in Tallinn in 2008, was established to promote cooperation, information sharing, and research in the field of cyber security. The Centre's sponsoring states are Estonia, Germany, Hungary, Italy, Latvia, Lithuania, Slovakia and Spain.[51]

Estonia has also created a Department of Critical Infrastructure Protection, tasked to defend public and private networks at the strategic level. They conduct risk assessments, collect information on critical infrastructure and propose defensive measures to counteract cyberthreats. Projects include mapping critical infrastructure, designing contingency plans and risk assessments for large-scale cyberattacks.[52]

## Finland

Finland's approach to cybersecurity has distributed the responsibility for cyberdefence throughout the government and military. Finland views cybersecurity as an issue that, in normal conditions, poses a greater threat to industry and business than to the military. Finland has called for improved cyber intelligence capabilities to track organized crime and terrorist threats against the country.[53] In the 2006 *Strategy for Security in Society*, Finland regarded cyberattacks or disruptions in industry and e-commerce as the most significant threats in the cyber domain during peacetime.[54] The Ministry of Transport and Communications is responsible for responding to cyber incidents in information communications and technology systems. The Ministry of Trade and Industry is responsible for national security if a cyber incident significantly disrupts the economy.[55]

Finland's Security and Defence Policy of 2009 cites cyberspace as an emerging area that must be secured to protect the government, military and private sector.[56] In March 2011 the Finnish Ministry of Defence called for Finland's first official cyber strategy doctrine as part of the implementation of the Strategy for Security in Society, a government resolution originally published in 2006. The Security and Defence Committee is now responsible for preparatory work related to a cyber strategy.[57]

## France

France's *White Paper on Defence and National Security*, issued in 2008 by the Ministry of Defence, highlighted the threat of large-scale cyberattacks against critical infrastructure as a prominent national security concern and defined new strategies for cyberdefence. In the document, France describes the cyber domain as an area in which its sovereignty

51 See NATO Cooperative Cyber Defence Centre of Excellence, <www.ccdcoe.org>.

52 "Estonia Country Report". European Network and Information Security Agency, <www.enisa.europa.eu/act/sr/files/country-reports/Estonia.pdf>, 2011, p. 20.

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

54 *The Strategy for Securing the Functions Vital to Society*, Finnish Government resolution 23.11.2006, p. 48.

55 Ibid., pp. 36ff.

56 *Finnish Security and Defence Policy 2009*, Prime Minister's Office of Finland, 2009, p. 56.

57 "Cybersecurity preparedness", Finnish Government Communications Unit, press release 68/2011, 8 March 2011, <www.valtioneuvosto.fi/ajankohtaista/tiedotteet/tiedote/fi.jsp?toid=1802&c=0&moid=1805&oid=323303>.

"must be expressed fully", and states that it is pursuing a two-pronged strategy in building its defensive and its offensive capabilities.[58]

The main authority for cyberdefence in France is the National Agency for the Security of Information Systems, which was established in 2009. Its missions include detecting and reacting to cyberattack, preventing cyber threats by supporting research and development, and providing information to government and critical infrastructure entities.[59] It operates under the Prime Minister and is supervised by the General Secretariat for National Defence. France is also developing an offensive cyberwar capability under the purview of the Joint Staff and specialized services.[60] Both the army and the air force have electronic warfare units.[61] Offensive capabilities are also being pursued by the intelligence services.[62]

In February 2011, the Network and Information Security Agency released the official French cyber doctrine. France's four objectives in cyberspace include becoming a global power in cyberdefence, guaranteeing information sovereignty and freedom of decision, securing critical infrastructure and maintaining privacy in cyberspace. Information sovereignty and international cooperation are emphasized.[63]

## Georgia

Georgia's Ministry of Defence's *Minister's Vision 2010* prioritizes the development of information and communications technology and information security to ensure the effective and secure flow of information at strategic, operational and tactical levels. The Ministry of Defence seeks to develop electronic warfare capabilities and train personnel to disrupt adversarial communication.[64] The National Security Concept (2005) sets the direction for national security policy and overall development of state institutions; it maintains the importance of the secure flow of information and the protection of classified information for preventing and resolving crises. [65]

## Germany

Germany recently issued a new doctrine on cybersecurity and is creating two organizations to counter cyberthreats. The German government plans to set up a national cyberdefence centre in 2011 under the Ministry of the Interior. The new centre will combine resources from various government agencies, including the federal police and foreign intelligence agency. It will also include participation from industry. The 2011 Strategy focuses on

58 Ibid., p. 10.

59 "France Country Report", European Network and Information Security Agency, 2010, <www.enisa.europa.eu/act/sr/files/country-reports/France.pdf>, pp. 5, 23.

60 "The French White Paper on Defence and National Security", 2008, <www.ambafrance-ca.org/IMG/pdf/Livre_blanc_Press_kit_english_version.pdf>, p. 3.

61 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; "Chapter Four: Europe", *The Military Balance*, vol. 111, no. 1, 2011, pp. 104–09.

62 "French White Paper on Defence and National Security", 2008, <www.ambafrance-ca.org/IMG/pdf/Livre_blanc_Press_kit_english_version.pdf>, p. 9.

63 See *Défense et sécurité des systèmes d'informations: Stratégie de la France*, National Network and Information Security Agency, 2011.

64 See "Minister's Vision 2010", Ministry of Defence of Georgia, <www.mod.gov.ge/files/wqawuvhmkpeng.pdf>, p. 5.

65 *National Security Concept of Georgia*, Ministry of Defence of Georgia, 2005, <www.mod.gov.ge/?page=-10&Id=3&lang=1>.

protecting critical information infrastructure, securing and strengthening IT systems, establishing a National Cyber Response Centre and National Cyber Security Council, improving law enforcement, promoting international engagement, ensuring reliable and trustworthy information technology, and training the cyber workforce.[66]

The National Cyberdefence Centre is primarily responsible for German's cybersecurity. It will report to the Federal Office for Information Security, and will have no have offensive capabilities.[67] The new facility will initially be staffed with six employees from the German security agency BSI as well as two each from the German Office for the Protection of the Constitution (the domestic intelligence agency) and from the Federal Office of Civil Protection and Disaster Assistance (BBK). In the future, the Federal Police, Federal Office of Criminal Investigation, the Bundesnachrichtendienst, the Bundeswehr and the Customs Criminal Investigation Office (ZKA) will all place experts at the defence centre. The National Cybersecurity Council will be responsible for coordinating defence techniques and cyber policy. Senior military representatives will be among the staff.[68]

German military units and intelligence agencies have cyber components. The Germany security agency BSI is investing in the research and development of cyber capabilities. The Department of Information and Computer Network Operations, within the Bundeswehr's Strategic Reconnaissance Unit of the Bundeswehr, is headed by an Air Force Brigadier General, with 76 military personnel from the Bundeswehr's own computer science departments and will develop both offensive and defensive capabilities.[69]

## India

In the late 1990s, the Indian army shifted policy to incorporate electronic warfare and information operations into its doctrine. This led to the modernization of four military elements—information technology, electronic warfare, critical infrastructure protection and army mobility.[70] In December 2009, senior Indian Army officers reiterated the need for India to develop the capability to counter asymmetric threats, specifically cyberthreats.[71]

India has multiple units within the Ministry of Defence responsible for cybersecurity. The Defence Information Warfare Agency coordinates information warfare responses.[72] The Defence Intelligence Agency and the National Technical Intelligence Communication Centre have been working to create a joint "cybersquad" that would hack legally to

66 *Cyber Security Strategy for Germany*, German Federal Ministry of the Interior, 2011.

67 Felix Knote, "De Maizière priest neue Cyber-Zentrale", *Der Spiegel*, 2 February 2011.

68 Ibid.; *Cyber Security Strategy for Germany*, German Federal Ministry of the Interior, 2011, pp. 8–10.

69 John Goetz, Marcel Rosenbach and Alexander Szandar, "National defense in cyberspace", *Der Spiege*l, 11 February 2009.

70 Charles Billo and Welton Chang, "Cyber Warfare: An Analysis of the Means and Motivations of Certain Nation States", Institute for Security Technology Studies, Dartmouth University, 2004, pp. 41–45.

71 "Network centricity: an answer to security threats", *SP's Land Forces*, <www.spslandforces.net/news/?id=16&h=Network-Centricity-:-An-answer-to-security-threats>.

72 Unconfirmed reports published in Indian and Pakistani newspapers in early 2003 describe the Defence Information Warfare Agency as the agency responsible for creating cyberpolicy and countermeasures for the army, naval, and air force intelligence branches. See also Vinod Anand, "Integrating the Indian Military: Retrospect and Prospect", *Journal of Defence Studies*, vol. 2, no. 2, 2008, p. 37.

alert the government to potential cyber vulnerabilities.[73] The Defense Research and Development Organization built two ranges for testing electronic warfare systems.[74]

In 2005, the Indian Army created the Cyber Security Establishment to secure networks at the division level and conduct security audits.[75] The army also established the Cyber Security Laboratory at the Military College of Telecommunications Engineering in April 2010.[76] The Research and Analysis Wing of the Prime Minister's Office is the main source of electronic intelligence. Within this wing, the National Technical Intelligence Communication Centre provides technical and electronic intelligence to different agencies and intercepts communication from adversaries.[77] More recently, India's National Security Advisory Board recommended the creation of central cybersecurity command modelled on the United States' Cyber Command. Currently, the National Technical Research Organisation, along with the Defence Intelligence Agency, are responsible for developing offensive cyber capabilities. India has also signed a non-binding memorandum of understanding with the United States that enables technical and operational cooperation to thwart cyberthreats.[78]

## Israel

Israel is deemed to have advanced offensive cyber capabilities, but Israel's cybersecurity doctrine and strategy are only vaguely described in open-source literature. Four organizations are responsible for Israeli cyber defences. The Israel Defense Forces' Unit 8200 is staffed by military conscripts and officers, and it focuses on three areas of cyberwar: intelligence gathering, defence and attack.[79] Since the late 1990s, Shin Bet has been responsible for defending government systems, national infrastructure and financial data.[80] The C4I Corps is responsible for communication and organizing cyberdefence capabilities. In 2009, to improve cooperation between Military Intelligence and C4I, a senior intelligence officer was assigned to the Centre for Encryption and Information Security (known as Matzov) with responsibility for providing intelligence on technological advances among Israel's adversaries in the field of computer hacking.[81] Matzov is responsible for writing the codes that encrypt Israel Defense Forces, Shin Bet and Mossad networks. The C4I Corps has teams that test firewalls and encryption.[82] Senior Israeli 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.[83]

---

73 Harsimran Singh and Joji Thomas Philip, "Spy game: India readies cyber army to hack into hostile nations' computer systems", *The Economic Times*, 6 August 2010.

74 "India to built two test ranges of electronic warfare systems", *Business Standard*, 24 November 2010.

75 Rajat Pandit, "Army gearing up for cyber warfare", *The Times of India*, 7 July 2005.

76 "Army sets up cyber security lab", *Governance Now*, 6 April 2010, <www.governancenow.com/news/regular-story/army-sets-cyber-security-lab>.

77 Charles Billo and Welton Chang, "Cyber Warfare: An Analysis of the Means and Motivations of Certain Nation States", Institute for Security Technology Studies, Dartmouth University, 2004, p. 48.

78 Josh Smith, "U.S. Signs Cybersecurity Pact with India", *Nextgov*, 19 July 2011.

79 Amir Oren, "IDF dependence on technology spawns whole new battlefield", *Haaretz*, 3 January 2010.

80 Yaakov Katz, "Security and defense: nuclear worming", *The Jerusalem Post*, 10 August 2010.

81 Ibid.

82 Ibid.

83 Ibid.

Israel created a new government agency, the National Cybernetic Taskforce, on 18 May 2011 to secure the country against hacking of critical networks as well as to protect private industry from espionage. It will be an 80-member team and operate in a defensive capacity.[84] The Taskforce will also devote resources to improving university research on cybersecurity and increasing the number of students.

## Iran

Iranian cyber capabilities are coordinated within the military by the Passive Defence Organization.[85] The Islamic Revolutionary Guard Corps has a cyberwarfare unit. This unit is estimated to have 2,400 staff and a budget of $76 million.[86] In 2010, a military commander described this as the second largest cyber army in the world, a comment many interpret as evidence that the Iranian army employs civilian hacker groups, such as the "Iranian Cyber Army".[87] The Iranian Cyber Police Unit, launched in 2011, is mainly used to police social media websites.[88] The Iranian Cyber Army is a group of hackers, which allegedly has links to the Revolutionary Guard and the Ashiyane hacker forum.[89] At minimum, all three groups have a good working relationship, and some speculate they share members and tactics.

Iran announced in June 2011 that it plans to establish a cybercommand for the state's armed forces to defend against cyberattack and centralize operations. Iranian officials claim that the cyber command will be defensive and that it will be primarily concerned with thwarting Western efforts to incite dissent within the country.[90]

## Italy

Italy is in the process of formulating its cyber strategy and improving its offensive cyber capabilities. The Italian military has an electronic warfare unit responsible for intelligence, surveillance, target acquisition and reconnaissance.[91] Additionally, the Telematics Section of the Carabinieri was established to combat cyber crime and terrorism.[92] Other elements monitoring cybersecurity include the Defence Innovation Centre and the Division for Information Security of the Defence Staff.

## Kazakhstan

The Kazakh Ministry of Communication and Information controls much of the country's centralized IT infrastructure. It has demonstrated the capability to control traffic and

84 "Eye on tech exports, Israel launches cyber command", *Reuters*, 18 May 2011.

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

86 Kevin Coleman, "Iranian cyber warfare threat assessment", *DefenseTech.* 23 September 2008. <http://defensetech.org/2008/09/23/iranian-cyber-warfare-threat-assessment/>.

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

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

89 Khashayar Nouri, "Cyber wars in Iran", *Mianeh*, 22 July 2010.

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

91 "Chapter Four: Europe", *The Military Balance*, vol. 111, no. 1, 2011.

92 "Italy Country Report", European Network and Information Security Agency, 2011, <www.enisa.europa.eu/act/sr/files/country-reports/Italy.pdf>, pp. 9–10.

access domestically.[93] These same capabilities could be used offensively. An agreement on civil nuclear cooperation with India also included a memorandum of understanding between the states' Computer Emergency Response Teams supporting coordination in the event of a mutual response to cyber incidents, the exchange of information on threats and attacks, and the exchange of human resources.[94]

## Malaysia

The Malaysian Ministry of Defence implements IT security policy to protect government and businesses from cyberattack. Among its missions are ensuring the safety of networks and preventing cyber incidents from having harmful economic impact. In 2007, the CyberSecurity Malaysia programme was launched by the Prime Minister at a meeting of the National Information Technology Council.[95] CyberSecurity Malaysia is part of the Ministry of Science, Technology and Innovation and runs a help centre for Internet users, a training centre for professionals, and keeps the public informed about cyberthreats. The agency is also involved in law enforcement to combat cybercrime.[96] After a series of cyberattacks against government websites June 2011, the Malaysian government has stated that it will introduce new laws pertaining to cybersecurity, including better encryption methods.[97]

## Myanmar

The Defense Services Computer Directorate, established in the 1990s to modernize the military, has shifted its mission to encompass network-centric warfare, cyber capabilities and electronic warfare. The army of Myanmar's military strategy was expanded to include cyberwarfare, as part of a "people's war under modern conditions".[98] There is speculation that the State Peace and Development Council (which controls the military) has obtained cyberwarfare technology from other Asian states.[99]

## The Netherlands

In early 2011 the Netherlands Government issued a National Cyber Security Strategy. 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 also calls for annual trend reports in cybercrime and digital security, and states that a National ICT [information and communications technology] Crisis Plan will be published in mid-2011. There is no

93 See "Kazakhstan", in Sanja Kelly and Sarah Cook (eds), *Freedom on the Net 2011*, Freedom House, 2011, pp. 214–223.

94 "India, Kazakhstan sign seven bilateral agreements", *Asian News International*, 16 April 2011.

95 "Corporate Overview", CyberSecurity Malaysia, <www.cybersecurity.my/en/about_us/brief_detail/main/detail/729/index.html?mytabsmenu=0>.

96 Ibid.

97 "Malaysia to introduce more laws to tackle cyber intrusion", *Press Trust of India*, 21 June 2011.

98 Aung Zaw, "Than Shwe's 'The Art of War'", *The Irrawaddy,* vol. 17, no. 2, 2009.

99 "Burma/Myanmar: How Strong is the Military Regime?", Asia Report no. 11, International Crisis Group, 21 December 2000; William Ashton, "Burma receives advances from its silent suitors in Singapore", *Jane's Intelligence Review*, 1 March 1998; David Scott Mathieson, "Book review: Strength and Dishonor: Building the Tatmadaw by Maung Aung Myoe", *Asia Times*, 4 July 2009.

additional funding for these initiatives, as the strategy states that the activities described in the Strategy "will be dealt with within the existing budgets".[100]

The Netherlands is developing new policies and agencies to counter cyberthreats. The National Cyber Security Board will develop strategy and policy, and is now operational.[101] The Ministry of the Interior coordinates interdepartmental cybersecurity between various civilian and military units responsible for cyber issues. The Ministry of Defence will cooperate on cyberdefence and has developed electronic warfare capabilities within the army.[102]

The government will begin working on a Cyber Security Agenda and Centre. The Netherlands will establish the National Cyber Security Centre to centralize cyber operations under one command. It is expected to be operational by January 2012.[103] 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.[104] There will also be a Cyber Education and Training Center to research cyberdefence and to develop the human capital necessary to bolster a growing digital economy. A starting date for this organization has yet to be set.[105]

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.[106] The Netherlands has signed a memorandum of understanding with Luxembourg and Belgium for cooperation in cybersecurity, including information- and expertise-sharing, and cooperation on best practices and the development of public–private partnerships.[107]

## Norway

Norway completed the drafting stage of the National Cyber Defence Strategy in 2010, and the legislative phase was to commence at the end of that year. The Strategy will be implemented by the Ministry of Defence.[108] The Strategy proposes 22 measures to strengthen Norway's ability to prevent and manage cyber events. The main objectives are the following: to establish a common situational overview and understanding of

100 "The National Cyber Security Strategy: Success Through Cooperation", Netherlands Ministry of Security and Justice, 2011.

101 This is referred to as the "National Cyber Security Board" in the National Cyber Security Strategy; in speeches by public officials it is sometimes referred to as the "National Cyber Security Council". Don Eijndhoven, "Dutch Cyber Security Council now operational", *Infosec Island*, 5 July 2011.

102 The army, as part of its Intelligence Signals and Reconnaissance forces, has one battalion that contains a company specializing in electronic warfare. Don Eijndhoven, "Dutch government to design cyber defense doctrine", *Infosec Island*, 27 February 2011.

103 "NCSC: Nationaal Cyber Security Centrum: Dutch National Cyber Security Centre is in the making", *CWZ*, 11 May 2011.

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

105 Ibid., p. 8.

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

107 "Benelux sign memorandum of understanding on cyber security", *European Urban Knowledge Network*, 12 April 2011.

108 Gerard O'Dwyer, "Norway drafts cyber defense initiative", *DefenseNews*, 27 January 2010.

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.[109]

## Poland

The Polish Defence Strategy identifies cyberattack as a dangerous asymmetrical threat.[110] Although Poland is seeking to improve its cyber capabilities, cyber has been relegated to a combat support function rather than a new method of warfare. However, Poland's *Vision of the Polish Armed Forces in 2030* seeks to change the role of cyber in the military and places a particular emphasis on cyber terrorism's threat to information resources and the Polish energy sector.[111] Poland will create a unit called the Independent Information Force within the army. This unit will integrate electronic intelligence, psychological operations, and cyber offensive and defensive actions across the military.[112] Progress in the creation and development of the Independent Information Force is unclear. Poland's NATO partnership is an important element of its cyber defence strategy. In February 2011, Poland signed an agreement with NATO Consultation, Command, and Control Agency that would facilitate the development of new technologies to counter cyber threats.[113]

## The Republic of Korea

The 2008 *Korean Defense White Paper* identifies cybersecurity as an essential component of national defence.[114] The 2010 *Defense White Paper* outlines cyberattack as one of several non-traditional security threats.[115] Computer emergency response teams have been created at the corps level to oversee the Defence Information Systems.[116] 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.[117]

The Ministry of National Defence has a Cyber War Centre, created in January 2010. Its primary aim is to increase the security of government and financial information networks.[118] The Defence Ministry also announced it would create an independent Cyber Warfare Command responsible for defensive and offensive operations in cyberspace.[119] The National Cybersecurity Strategy Council is the coordinating body for developing cyber policy, and is chaired by the head of the National Intelligence Services. Advising the

109 "Proposed Strategy for Cyber Security", Norwegian Ministry of Defence, 21 December 2009, <www.regjeringen.no/nb/dep/fd/dok/hoeringer/hoeringsdok/2010/forslag-til-strategi-for-cybersikkerhet/Horingsnotat.html?id=599898>.

110 *Defense Strategy of the Republic of Poland*, Ministry of National Defense, 2009, <www.wp.mil.pl/pliki/File/English/strategia_obronnosci_eng.pdf>, p. 5.

111 *Vision of the Polish Armed Forces in 2030*, Ministry of Defense Department of Transformation 2008 <http://www.wp.mil.pl/pliki/File/vision_of_paf_2030.pdf>, p. 14.

112 Ibid., p. 24.

113 "Poland signs advanced technology agreement with NC3A", NATO C3 Agency, 24 February 2011.

114 *Defense White Paper: 2008*, Ministry of National Defence, Republic of Korea, pp. 192–219, 222.

115 *2010 Defense White Paper*, Ministry of National Defence, Republic of Korea, 2010, pp. 8–10.

116 Ibid., pp. 164–65.

117 Ibid.

118 Ibid.

119 "Cyber Security Is Vital for National Defense", *Chosunilbo*, 2 November 2009, <http://english.chosun.com/site/data/html_dir/2009/11/02/2009110200788.html>.

Council is the Korea Internet Security Centre, a public–private partnership with the Korea Communications Commission.[120] The military and Korea University will collaborate in the creation of a cyberwarfare school where students will be trained to deal with a variety of cyber threats. Upon graduation, the students will become military officers working in cyberwarfare units.[121]

## The Russian Federation

In February 2010 the Russian Federation released its new military doctrine, which discusses the use of political and informational instruments to protect Russia's national interests and those of its 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. The doctrine states that the "Early implementation of measures of information warfare to achieve political objectives without the use of military force, and in the future to generate a favorable reaction of the international community to use military force" will be a characteristic of future conflict. The task of equipping the armed forces and other troops includes "the development of the forces and means of information warfare", and "the creation of new types of precision weapons and the development of their information security" as part of "the information space of the Russian Federation".[122]

Previously, information warfare was defined in 1997 by the Federal Agency of Government Communications and Information as having four components: the destruction of command and control centres and electromagnetic attack on information and telecommunications systems; the acquisition of intelligence; disruption of computer systems; and disinformation.[123] The Federal Security Service in 2003 absorbed parts of the Federal Agency of Government Communications and Information, which had been responsible for cryptology and code-breaking.[124] Russia maintains strong partnerships with industry and universities to assist with the research and development of cyber capabilities.

## Switzerland

The Report on the Security Policy of Switzerland of June 2010 recognizes both the importance of critical infrastructure and its vulnerability to cyberattack. To defend against this threat, Switzerland seeks to improve its cyberdefences.[125] 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 Computer Emergency Response Team, which will be tasked to monitor the systems and networks of the armed forces. It will coordinate

120 Terrence Park, "Korean Cybersecurity Framework", presentation at the 2009 ITU Regional Cybersecurity Forum for Asia–Pacific, 23 September 2009, <www.itu.int/ITU-D/cyb/events/2009/hyderabad/docs/park-korean-cybersecurity-framework-sept-09.pdf>.

121 Jamie Yap, "South Korea army, university to start cyberdefense major", *ZDNet*, 29 June 2011; see also "South Korea to open cyber warfare school", *Physorg.com*, 29 June 2011.

122 "Военная доктрина Российской Федерации", Russian Presidential Executive Office, 5 February 2010, <http://news.kremlin.ru/ref_notes/461>.

123 "Cyber Wars", *Agentura.Ru*, <www.agentura.ru/english/equipment/>.

124 Roland Heickerö, "Emerging cyber threats and Russian Views on Information Warfare and Information Operations", Swedish Defence Research Agency, 2010, pp. 27ff.

125 *Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz*, Swiss Federal Council, 23 June 2010, pp. 5, 14.

with the government Computer Emergency Response Team.[126] The other is a unit for computer network operations. The Federal Department of Defence intends to develop computer defence, exploitation and attack capabilities.[127]

## Turkey

The Turkish National Security Council has approved a new national strategy, adding cybersecurity threats for the first time. Turkey's military strategy, popularly termed the "Red Book", was revised in October 2010 to include cyber threats, among other non-conventional threats.[128]

Turkey plans to establish a Cyber Army Command to counter cyberattacks 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 of Turkey and Middle East Technical University.[129] Despite the fact that it will be subordinated to the General Staff, Turkey's cyber army will have its own budget and an autonomous structure. The command will monitor the entire Internet network in Turkey and offer protection to state institutions.[130]

Turkey has also merged two agencies to create a single entity, BILGEM, that is tasked to intercept signals and secure Turkey's electronic communications. This new entity will be staffed by researchers who will study cryptography, cybersecurity, electronic warfare, and develop software for the public and private sectors.[131]

## The United Kingdom

The *Cyber Security Strategy of the United Kingdom*, released in June 2009, contains a three-pronged approach: reducing risk, exploiting opportunities and improving the response to cyber incidents. Reducing risk in cyberspace entails reducing vulnerability to and mitigating the impact of cyber incidents. The United Kingdom will gather intelligence, promote government policies, and take action against adversaries. Lastly, improving response entails improving knowledge and awareness, developing doctrine and policy, improving governance and decision-making structures, and enhancing technical and human capabilities.[132]

The 2010 National Security Strategy highlights "[h]ostile attacks upon UK cyber space by other states and large scale cyber crime" as among the highest priorities for national

126 See "Gutachten über Rechtsgrundlagen für Computernetzwerkoperationen durch Dienststellen des VBS", 2 Septermber 2009, <www.parlament.ch/d/organe-mitglieder/delegationen/geschaeftspruefungsdelegation/gutachten-zhd-gpdel/Documents/gutachten-ejpd-computernetz-vbs-2009-03-10-d.pdf>.

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

128 "New edition of Turkish Red Book shapes new security spheres", *Hürriyet Daily News*, 28 October 2010.

129 Ercan Yavuz, "Turkey to mobilize against cyber-terrorism", *Today's Zaman*, 30 January 2011.

130 Ibid.

131 "Turkey creates its own 'NSA'", *TR Defence*, 09 September 2010.

132 *Cyber Security Strategy of the United Kingdom*, UK Office of Cyber Security, 2009, p. 4.

security.[133] According to the Strategic Defence and Security Review of 2010, the United Kingdom allocated £650 million over four years (2009–2013) for these initiatives.[134]

The Cyber Security Operations Centre is responsible for developing both offensive and defensive cyber capabilities. Its primary tasks are to monitor the development and health of government IT systems, analyze trends and improve responses to cyber incidents.[135] The Centre was scheduled to be operational in early 2011, with an initial staff of 19.[136] The Centre did not have a budget in FY 2009–2010, and the Government Communications Headquarters, the Cabinet, and security and law enforcement agencies paid for its initial costs.[137]

The Office of Cyber Security and Information Assurance coordinates government policy and strategy within the Cabinet Office. It is focused on supporting cyber education and awareness and promoting international engagement.[138] The Director of the Office reports to the National Security Advise.[139] The operating budget of the Office for FY 2009–2010 was £130,000.[140] The United Kingdom is planning to invest $1.06 billion over four years in its cybersecurity efforts.[141]

## The United States

The United States has focused on cybersecurity since the 1990s. Responsibility is divided between the Department of Homeland Security, the Federal Bureau of Investigation, and the Department of Defense, including the new US Cyber Command (which has the National Security Agency as one of its components). Offensive operations are most likely assigned to Cyber Command and to elements of the Central Intelligence Agency.

The Department of Homeland Security has primary responsibility for domestic defence. Its National Cyber Security Division is tasked to "work collaboratively with public, private, and international entities to secure cyberspace and America's cyber interest".[142] The Division also has a number of programmes to protect cyber infrastructure from attack.[143] 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

133 *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, UK Prime Minister's Office, 2010, p. 27.

134 Ibid., p. 47.

135 *Cyber Security Strategy of the United Kingdom*, UK Office of Cyber Security, 2009, p. 17.

136 "Delay in start date for U.K. cyberdefense center", *Homeland Security News Wire*, 12 March 2010.

137 UK House of Lords, Hansard, vol. 714, part no. 134, 11 November 2009, column WA173, <www.publications.parliament.uk/pa/ld200809/ldhansrd/text/91111w0004.htm>.

138 "Office of Cyber Security and Information Assurance", UK Cabinet Office, <www.cabinetoffice.gov.uk/content/office-cyber-security-and-information-assurance-ocsia>.

139 See "Structure charts - Cabinet Office", UK Cabinet Office , <www.cabinetoffice.gov.uk/resource-library/structure-charts-cabinet-office>.

140 Tom Espiner, "UK cybersecurity centre starting operations in March", *ZDNet*, 13 November 2009.

141 Eleanor Keymer, "UK recruits cyber experts to protect key networks", *Jane's Defence Weekly*, 6 February 2011.

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

143 See *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*, 17 December 2003.

nationally significant cyber incident.[144] The Group operates under the National Cyber Security Division.

Cyber Command, a military subcommand under US Strategic Command, is responsible for dealing with threats to the military cyber infrastructure. Cyber Command's service elements include Army Forces Cyber Command, the Twenty-fourth Air Force, Fleet Cyber Command and Marine Forces Cyber Command.[145] In order to facilitate cooperation, the Department of Defense and the Department of Homeland Security signed a memorandum of agreement on cybersecurity in October 2010 to increase interdepartmental collaboration.[146]

The *Cyberspace Review Policy*, completed in 2011, outlines a the roles of federal agencies to secure cyber infrastructure. In the short term, the Executive branch is expected to appoint new cybersecurity officials and increase awareness within the federal government of existing threats.[147] Many of the points in the *Cyberspace Review Policy* are also found in the 2010 *National Security Strategy*.[148] The May 2011 *International Strategy for Cyberspace* states that the United States "reserves the right to use all necessary means" to defend itself and its allies and partners, but that it will "exhaust all options before [the use of] military force".[149]

## Ukraine

Although Ukraine has developed cyber capabilities pertaining to security and law enforcement, its military cyber capabilities and doctrine are unclear. 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.[150]

The military's involvement in dealing with cyberthreats is outlined in a white paper entitled Ukraine's Strategic Defence Bulletin until 2015. 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".[151] Ukraine is part of a working group with NATO on cyber and military reform.[152]

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

145 "U.S. Cyber Command Fact Sheet", US Department of Defense, <www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPD>.

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

147 *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, The White House, May 2009, p. 37.

148 *National Security Strategy*, The White House, May 2010.

149 *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, The White House, May 2011, p. 14.

150 Vladimir Golubev, "Fighting cybercrime in CIS: strategy and tactics", Computer Crime Research Center, 29 June 2005.

151 "Ukraine's Strategic Defence Bulletin until 2015", defence white paper, 2004, p. 16.

152 *White Book 2007: Defence Policy of Ukraine*, Ukraine Ministry of Defence, 2008, p. 109.

# Civil Policy and Organizations for Cybersecurity

## Antigua and Barbuda

Antigua and Barbuda views cybersecurity as an important national security issue. It is working to improve cybersecurity through education, research, training and technology development. Antigua and Barbuda seeks to play a leading regional role in cybersecurity.[153] On 12–15 July 2009, Antigua and Barbuda held the First National Workshop on Cyber Security and Incident Response. The workshop's objectives, and the objectives of the government of Antigua and Barbuda, were to conduct a national security self-assessment in order to identify vulnerabilities particular to the cyber domain, and to create a governmental Cyber Security Incident Response Team. Antigua and Barbuda is already home to a Regional Cyber Forensics Lab that assists in regional cyber law enforcement, and has started training police officers in cybercrime investigation.[154]

## Belgium

Responsibility in the Belgian government for cyberdefence is spread among different departments and there is no central national authority. The Belgian Network for Information Security, a consultative platform in which many government institutions participate, advises the government on cyberthreats and critical infrastructure protection.[155] The *Modernization Plan 2000–2015 of the Belgium Armed Forces* cites "Increased computerised actions" as one of the four reasons for the creation of a unified join staff.[156] Belgium has signed a memorandum of understanding with the Netherlands and Luxembourg for cooperation in cybersecurity, including information- and expertise-sharing, and cooperation on best practices and the development of public–private partnerships.[157]

## Brunei Darussalam

The Brunei Computer Emergency Response Team was formed in May 2004 in collaboration with the Ministry of Communication. It coordinates with local and international computer emergency response teams as well as business, government agencies and Internet service providers.[158] The Authority for Info-Communications Technology Industry is the state's telecommunications and radio frequency regulator and is responsible for the development of information infrastructure.[159] The government focuses on employing cyber capabilities defensively, protecting internal systems and promoting information technology

153 "Antigua and Barbuda will be represented at cyber crime workshop", 19 April 2011, <http://ab.gov.ag/gov_v4/article_details.php?id=1381&category=38>.

154 Remarks by Lt. Col. Edward H.Croft at the First National Workshop on Cyber Security and Incident Response, 12–15 July 2010, <http://ab.gov.ag/gov_v4/pdf/speeches/remarks_by_edwardH_croft.pdf>.

155 "Country Report: Belgium", European Network and Information Security Agency, 2009, p. 15.

156 Jan Ondrejka and Richard Stojar, "Belgian Armed Forces: Trends in Development" Defence and Strategy, vol. 2003, no. 2, 2003, p. 112.

157 "Benelux sign memorandum of understanding on cyber security", *European Urban Knowledge Network*, 12 April 2011.

158 "About BruCERT", Brunei Computer Emergency Response Team, <www.brucert.org.bn>.

159 Authority for Info-Communications Technology Industry, <www.aiti.gov.bn/about/about_us.html>.

development.[160] Although the Ministry of Defence is not the agency responsible for cybersecurity, the military is committed to using information and computer technology to improve its diplomatic and defensive capabilities.[161]

## Bulgaria

Bulgaria aims to develop its domestic cyber capabilities while concurrently engaging the international community on cybersecurity issues. Bulgaria has signed a memorandum of understanding with NATO on fostering international collaboration to counter cyberthreats through information- and capability-sharing, as well as joint participation in cyber exercises. The Institute for Parallel Processing of the Bulgarian Academy of Science is a member of the EU SysSec Project, an international research consortium that studies emerging cyber threats.[162]

Bulgaria has four main tasks in the realm of cybersecurity: defining policies, creating mandates, producing recommendations, and training and educating citizens.[163] In 2010, the Deputy Defence Minister alluded to a National Cyber Authority, comprised of reserve officers and specialists from the IT community. This unit would share information and offer cyber training and education programmes.[164] A Ministry of Defence white paper states that Bulgaria is focusing on consolidating its information networks "so as to build a single information network".[165] This interconnectedness will require "vigilance on the part of military formations for its maintenance and security".

## Croatia

In January 2011, 19 ministries and government agencies met for a roundtable discussion of the Croatian National Security Strategy. Many voiced concerns that the most significant issue missing from the National Security Strategy was a policy for cybersecurity, responding to cybercrime and protecting digital infrastructure.[166] According to the Ministry of Defence's *Strategic Defence Review*, Croatia will be creating a Signals Unit that will be responsible for a stationary, network-information and encryption signal systems.[167]

160 "Brunei Darussalam Public Sector Journey Towards E-Government", 12th ACCSM Main Conference, 13–15 October 2003, <www.bruneiresources.com/pdf/accsm12_brunei_countrypaper.pdf>.

161 See Brunei Ministry of Defense, <www.mindef.gov.bn>; and Brunei Computer Emergency Response Team, <www.brucert.org.bn>.

162 See the project's website at <www.syssec-project.eu>.

163 Minchev Zlatogor, "New Threats in CyberSpace", presentation for the Round Table: Status and Problems of Security in Cyberspace of Bulgaria. Sofia, 28 September 2010, <www.atlantic-bg.org/images/news/round-table-cyber-sec-28_09-2010/docs/new-threats-in-cyber-space-zm-28-09-10.pdf>.

164 Address by the Deputy Minister of Defence Valentin Radev at the Round Table: Status and Problems of Security in Cyberspace of Bulgaria. Sofia, 28 September 2010, <www.atlantic-bg.org/images/news/round-table-cyber-sec-28_09-2010/docs/radev-privetstvie-28-09-10.pdf>.

165 White Paper on Defence and the Armed Forces of the Republic of Bulgaria, Bulgarian Ministry of Defence, <www.md.government.bg/en/doc/misc/20101130_WP_EN.pdf>, p. 43.

166 "Second roundtable on the draft of National Security Strategy", Croatian Ministry of Defence, 14 January 2011.

167 *Strategic Defence Review*, Croatian Ministry of Defence, 2005, <http://arhiva.morh.hr/katalog/documents/spo_eng.pdf>, p. 27.

## Cuba

Press reports suggest that Cuba, with Russian assistance, began looking at cybesecurity in the 1990s. The Cuban government holds a monopoly on telecommunications and controls internet traffic. It employs surveillance and security software to monitor internet access points.[168] Cuba portrays its efforts as defensive measures in line with its overall defensive military posture. The Ministry of Informatics and Telecommunications has prioritized the development of indigenous information technology to enhance cyber self-sufficiency and cybersecurity from potential external threats.[169]

## Cyprus

Cyprus's activities have focused on protection of personal information and cybercrime. In 2004, Cyprus passed a cybercrime law covering illegal access, data interception or interference, misuse of devices, and computer forgery and fraud. The law also ratified the Convention on Cybercrime. CyberEthics, a partnership among government agencies, the press and Internet service provider associations, allows police to work with private companies in investigating cybercrime incidents.[170] Two national CERTS (one for government, and one for academia and the private sector) were established in 2010.[171]

## The Czech Republic

The Czech Republic's 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.[172] The Czech Republic is increasingly focused on cybersecurity after losing more than €10 million in a cyberattack on the European Union Emissions Trading System.[173] In March 2010 the Czech Republic assigned the Ministry of Interior to coordinate cybersecurity issues, develop interdepartmental coordination, and establish a Computer Emergency Response Team.[174] According to the Ministry of Defence, the upcoming 2011 Defense White Paper will lay down cybersecurity priorities, but no specific projects and no new funds have been put in place for cyberdefence.[175]

168 See "Cuba", in Sanja Kelly and Sarah Cook (eds), *Freedom on the Net 2011*, Freedom House, 2011, pp. 6, 24.

169 See "Doctrina Militar Cubana", Cuban Ministry of the Revolutionary Armed Forces, <www.cubagob.cu/otras_info/minfar/doctrina/doctrina_militar.htm>; and "Fighting cyber-attacks is a matter of national security: Cuban minister", *Xinhua*, 25 February 2011.

170 "Cyprus Country Report", European Network and Information Security Agency, 2011, <www.enisa.europa.eu/act/sr/files/country-reports/Cyprus.pdf>, pp. 7–8, 12.

171 Ibid., p. 13.

172 "Czech Republic Country Report", European Network and Information Security Agency, 2011, <www.enisa.europa.eu/act/sr/files/country-reports/Cyprus.pdf> pp. 5, 13.

173 Cat Contiguglia, "Global cyber security starts close to home", *The Prague Post*, 9 February 2011.

174 Through resoltuion 205 of 15 March 2010; see <http://racek.vlada.cz/usneseni/usneseni_webtest.nsf/0/B76A28558E43BEE6C12576E4003F0505/$FILE/205%20uv100315.0205.pdf>.

175 Ibid.

## Ghana

Ghana's intention of becoming the information hub of Western Africa has led the government to enact cybercrime legislation and enhance cybersecurity practices.[176] The Electronic Communications Act and the Electronic Transactions Act govern the legal framework for governing information technology in Ghana.[177] The Ministry of Communications announced in 2009 that it would develop a computer emergency response team to monitor and respond to cybercrime in collaboration with security agencies.[178]

## Hungary

Hungary defines national security as including cyberdefence.[179] The National Cybersecurity Center is tasked with protecting central government systems as well as critical infrastructure from cyberattack.[180] The Center focuses on prevention and early detection of cyberattacks and is developing the technical capability to defend against them. 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 fora in cybersecurity exercises and information-sharing initiatives. It is part of the Prime Minister's Office and is led by the Information Security Supervisor of the Government.[181]

## Indonesia

Indonesia's military does not have cyberwarfare capability, and the government has not released a cyber doctrine or strategy.[182] However, Indonesia has started drafting cyber legislation. These efforts have included Indonesia's cybercrime legislation, which was developed in conjunction with the Council of Europe and focuses on maintaining the security of electronic transactions and preventing data interference and theft of personal

176 Joseph Coomson, "Ghana: cyber crimes in Ghana", *Ghanaian Chronicle*, 6 October 2006, <http://seclists.org/isn/2006/Oct/30>.

177 Electronic Transactions Act, 2008, Parliament of the Republic of Ghana, 18 December 2008, <www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/WPFD2009/pdf/Ghana%20Electronic-Communications%20Act%202008.pdf>; "GIFEC In History", Ghana Investment Fund for Electronic Communications, <http://gifec.gov.gh>.

178 "Ghana to introduce cyber security bill to check cyber crimes", *Ghana Business News*, 19 May 2009; Masahudu Ankiilu Kunateh, "Gov't to set up Computer Emergency Response Team to combat cyber srime in Ghana", *GhanaDot.com*, 17 June 2009.

179 *National Security Strategy of the Republic of Hungary*, Government of Hungary, 2004, <http://merln.ndu.edu/whitepapers/Hungary_English-2004.pdf>, pp. 1–2.

180 "About Us", PTA-CERT Hungary: National Cybersecurity Center, <www.cert-hungary.hu/en/node/6>.

181 "Hungary Country Report", European Network and Information Security Agency, 2010, <www.enisa.europa.eu/act/sr/files/country-reports/Hungary.pdf>, pp. 16, 25–26.

182 Rizal Sukma, "Indonesia's Security Outlook, Defense Policy, and Regional Cooperation", in *Asia Pacific Countries' Security Outlook and Its Implications for the Defense Sector*, The National Institute for Defense Studies, Japan, 2010.

information.[183] A new cybercrime bill called the Information Technology and Offense (RUU TIPITI) Bill was introduced in 2010.[184]

## Japan

The Japanese government has incorporated cyber capabilities in its emergency response planning and operations. Japan is beginning to create new organizations and fund research on cyber capabilities. The National Information Security Center, established in 2005, is responsible for national security and emergency response systems, including guarding against cyberattacks. The Center drafts standards, formulates recommendation and reports to the Cabinet Secretariat.[185] The Center's work 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. As part of the 2009 information technology security doctrine, all government agencies must assist the Team in improving cyberdefences.[186]

The Command, Control, Communications, and Computer Systems Command of the Japan Self-Defence Forces was established in 2008. It seeks to develop cyberdefence capabilities at the national level, and it is projected that future elements of this unit will have active defence capabilities against cyber adversaries. Within this command is the Cyberspace Defence Unit.[187] It will be operational in FY2012, and will seek to integrate cyberdefence into the military, coordinate, provide technical and training assistance, and research cyberwarfare options. In 2010, a Coordinator for Cyber Planning to be assigned to the Joint Staff was allocated in the defence budget.[188]

Japan's Ministry of Internal Affairs and Communications has also begun adopting cyberdefences. It established in 2006 the "Cyber Clean Center", a joint project with the Ministry of Economy, Trade and Industry. The Cyber Clean Center's primary function is to study botnets, analyzing their occurrence, countermeasures and infection programmes. Internet service providers and security vendors are assisting with this research.[189]

Japan's 2010 defence white paper highlighted cyber activity as a new development in warfare and described trends in the adoption of cyber capabilities.[190] In June 2011, Japan

183 "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>.

184 Warief Djajanto Basorie, "Indonesia's press freedom: regaining the other half", *The Jakarta Post*, 9 February 2011.

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

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

187 Yoshihiro Yamaguchi, "Development of JSDF Cyber Warfare Defense Critical Capability", US Air Command and Staff College, 2010, pp. 5–7.

188 "Defense Programs and Budget of Japan: Overview of FY2010 Budget", Japanese Ministry of Defence, 2009, <www.mod.go.jp/e/d_budget/pdf/220416.pdf>, p. 17.

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

190 *Defense of Japan 2010*, Ministry of Defence, part I, chp. 1, § 3.

and the United States announced a bilateral strategic policy dialogue on cybersecurity issues.[191]

## Jordan

The Jordanian Armed Forces have begun to install a Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) system to enhance interoperability between the armed forces and allies.[192] In 2010, the Jordanian Cabinet 2010 approved the Information System Crimes Law (Cyber Crime Law), issued by the Ministry of Information and Communication Technology.[193] The National Centre for the Security and Assurance of Information and Communication Systems of the Hashemite University has three e-crime labs to train students on combating cybercrime.[194]

## Kenya

Cybersecurity is an increasingly important issue as Kenya gains access to high-speed internet connections.[195] The Ministry of Information and Communication is developing a computer incident response team to coordinate responses to cyber incidents at the national level and to cooperate with regional and international bodies.[196] The Kenya Armed Forces Technical College trains technicians for the armed forces to operate and service information systems and equipment.[197]

## Latvia

Latvia passed an IT security law, which took effect in February 2011. The law creates a new IT security head for every agency. Two existing computer security agencies will be merged into a new Cyber-Security Response Agency, which will initially consist of eight IT experts.[198] The Latvian Ministry of Transport is the government entity responsible for information security policy development.[199] Latvia is a signatory of the Convention on Cybercrime and a series of criminal laws entered into force in Latvia in 1999 in order to combat cybercrime.[200]

Latvian defence documents describe information superiority in terms of surveillance, intelligence and secure communication networks as a priority combat capability.[201] The

191 Marcus Weisgerber, "Japan, U.S. To Expand Missile Defense, Cyber Cooperation", *DefenseNews*, 21 June 2011.

192 "Armed Forces (Jordan)", *Jane's*, <http://articles.janes.com/extracts/extract/emedsu/jords100.html>.

193 Rami Olwan, "New cyber crime law in Jordan", 13 August 2010.

194 Mohammad Ghazal, "Local cyber crime centre to serve region", *Jordan Times*, 16 February 2011.

195 Philip Ngunjiri, "Cyber crime a real threat as cables land", *The East African*, 18 May 2009.

196 "Information Security", Communications Commission of Kenya, <www.cck.go.ke/industry/information_security/certification_service_providers.html>.

197 Kenya Armed Forces Technical College, <www.mod.go.ke/airforce/?page_link=kaftec>.

198 "New Latvian data protection law to take effect Feburary 1", *Deutsche Welle*, 25 January 2011.

199 "Latvia Country Report", European Network and Information Security Agency, 2011, <www.enisa.europa.eu/act/sr/files/country-reports/Latvia.pdf>, p. 9.

200 Edward Lestrade, "The Cybercrime Phenomenon and Latvian Cybercrime Law", *European Newsletter, Doing Business in Europe*, 2006, pp. 4–5.

201 *The State Defence Concept*, Latvian Ministry of Defence, 2008, <http://doc.mod.gov.lv/en/Brosuras/valsts_aizsardzibas_koncepcija/files/publication.pdf>, pp. 4, 6 and 7.

Communications and Information System Command is tasked with ensuring the operation and development of the armed forces' communications and information infrastructure and ensuring its computer network maintains NATO security standards.[202] Latvia is a founding member of the NATO Cooperative Cyber Defence Centre of Excellence and regularly participates in cybersecurity exercises with other Baltic and NATO states.[203]

## Lithuania

Lithuania is developing a cybersecurity strategy and national laws for cybersecurity. It is a founding member of the NATO Cooperative Cyber Defence Centre of Excellence. It is highly involved in the NATO cyberdefence process and partners with other Baltic and NATO nations in regular cybersecurity exercises.[204] Lithuania's national cybersecurity strategy was developed by the Ministry of Defence.[205]

## Luxembourg

The Luxembourg national cyber strategy was launched in 2003 by the Ministry of the Economy and Foreign Trade. The strategy has four elements: enhancing public awareness and preventive measures, recovery capabilities, and investigation and forensics.[206] The Cyberworld Awareness and Security Enhancement Structure promotes awareness and proper IT security practices for citizens, businesses, and government. This body makes recommendations and provides information on vulnerabilities and threats to the national computer emergency response team and the Computer Incident Response Center Luxembourg.[207] Luxembourg has signed a memorandum of understanding with the Netherlands and Belgium for cooperation in cybersecurity, including information- and expertise-sharing, and cooperation on best practices and the development of public–private partnerships.[208]

## The Maldives

The Maldives National Defence Force and the Police Service have called for a comprehensive cyber strategy and legislation.[209] With assistance from the US Federal Bureau of Investigation, the Maldives Police Service has started a Cyber Crime Project to investigate cybercrime.[210] The Maldives is party to the Tonga Declaration, which was made by Pacific Information and Communication Technology Ministers to emphasize

202 "Report to the Parliament on National Defence Policy and National Armed Forces Development in 2006", Latvian Ministry of Defence, 2006, p. 39.

203 James Stavridis, "Effective Partnering for Cyber Security",*EUCOMversations: Official Blog of United States European Command,* 31 May 2011.

204 "Representatives of National Defence System will take part in international conference on cyber conflict in Tallinn", Ministry of National Defence Republic of Lithuania, 16 June 2010.

205 "Lithuania Country Report", European Network and Information Security Agency, 2011, pp. 5, 13.

206 "Luxembourg Country Report", European Network and Information Security Agency, 2011, p. 5.

207 Ibid. pp. 10–11.

208 "Benelux sign memorandum of understanding on cyber security", *European Urban Knowledge Network*, 12 April 2011.

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

210 "Maldives Police Service launches Cyber Crime Project", *Miadhu*, 20 May 2008.

the importance of such technology for development and regional cooperation on the issue, and has held additional sessions on cybersecurity and cybercrime legislation.[211]

## Malta

The Malta Information Technology Agency is responsible for implementing out the National Strategy for Information Technology.[212] The Malta Communication Authority is tasked with improving information infrastructure, expanding internet access and promoting e-commerce.[213] The 2010 "The Smart Island" strategy calls for a National Information Security Strategy to be implemented by a new National Information Security Agency. The Cyber Crime Unit of the Malta Police Force is responsible for investigating cybercrime and attacks on computer systems.[214] The Malta Information Technology Agency is updating the computer emergency response team, which will serve as a central point of contact for cyber incidents and threats. There is no formal cybersecurity body within the Armed Forces of Malta.[215]

## Morocco

Morocco's recent national strategy, *Digital Morocco 2013*, emphasizes cybersecurity as an economic benefit to ensure commerce and foster "cyber-confidence".[216] Morocco has signed a memorandum of understanding on cybersecurity with Malaysia, covering the areas of critical information infrastructure protection, cybersecurity frameworks development, capacity-building, training and awareness.[217]

## New Zealand

New Zealand has launched several initiatives to promote cybersecurity. Examples include Netsafe, an organization that aims to educate and raise awareness of cyberthreats, and the ORB (Online Reporting Button), a website through which citizens can report unlawful online activity.[218] The Ministry of Economic Development is the lead agency for cyber security policy. The Centre for Critical Infrastructure Protection is a government agency that worked with critical national infrastructure organizations and industry to improve cybersecurity and protection against cyber threats.

New Zealand will create National Cyber Security Centre in the Government Communications Security Bureau. It will absorb the current functions of the Centre for Critical Infrastructure Protection and expand existing cybersecurity and information assurance capabilities to protect government systems and information from advanced persistent threats. The Government will engage private critical infrastructure entities to improve cybersecurity,

211 "Need for regional cyber-security pushed in Nuku'alofa", Taimi Media Network, 29 April 2011.

212 "Malta Country Report", European Network and Information Security Agency, 2010, <www.enisa.europa.eu/act/sr/files/country-reports/Malta.pdf>, p. 5.

213 Ibid., p. 6.

214 Ibid., pp. 6–7.

215 Ibid., p. 15.

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

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

218 "Cyber Security Policy", Ministry of Economic Development. http://www.med.govt.nz/templates/ContentTopicSummary____45639.aspx

including the possible creation of a New Zealand Computer Emergency Response Team.[219] The Defence White Paper 2010 focuses on cyberwarfare as a growing threat to which New Zealand must respond.[220]

## Nigeria

Nigeria is very concerned with the negative effects of cybercrime on its economy. A National Cybersecurity Initiative, created by a Presidential Committee, was tasked to create cybersecurity recommendations. They issued three main recommendations: raise awareness on cybercrime, pass new legislation criminalizing certain cyber activities, and build Nigeria's institutional capacity to combat cybercrime. In 2004, the Nigerian Cybercrime Working Group was established to implement these recommendations within a two-year timeframe. The Working Group included members of law enforcement, government ministries, intelligence officials, and private sector representatives. After two years, the Directorate for Cybersecurity was created within the Office of the National Security Advisor, to continue to update Nigerian cyberpolicy and to coordinate these efforts.[221]

## Oman

Oman created a national Computer Emergency Readiness Team (OCERT) in 2010. It is located at an information technology park on the outskirts of the capital, called Knowledge Oasis Muscat. OCERT forms a command and control centre to coordinate cyber responses and issue safety advisories. They are also responsible for maintaining public IT infrastructure and securing financial transactions.[222]

## Pakistan

In 2007, Pakistan passed the Electronic Crime Ordinance issuing stringent rules on the use of the internet.[223] The National Response Centre for Cyber Crimes of Pakistan's Federal Investigation Agency seeks to enhance the government's capacity to prevent and investigate cybercrime, secure information resources and provide timely information to departments and critical infrastructure owners about cyberthreats and recovery techniques. The Centre, created in 2003, is the focal point for international collaboration and gathers cybersecurity intelligence. It pursues cases of credit card fraud, distributed denial of service and virus attacks, and financial crimes.[224] There is an active hacker community in Pakistan, and Pakistani groups have demonstrated an interest in cyber capabilities.[225]

---

219 *New Zealand's Cyber Security Strategy*, New Zealand Government, 2011, pp. 8–9.

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

221 Basil Udotai, "National Cybersecurity Strategies: Case Study–Nigeria", presentation at the Africa Regional Conference on Cybersecurity, Yamousoukro, 17–20 November 2008.

222 "Oman unveils cyber-security outfit", *Gulf News*, 5 April 2010.

223 Irfan Ahmed, "New cyber law in Pakistan restricts free speech", *OneWorld South Asia*, 24 January 2008.

224 National Response Centre for Cyber Crimes, <www.fia.gov.pk/prj_nr3c.htm>.

225 Charles Billo and Welton Chang, "Cyber Warfare: An Analysis of the Means and Motivations of Certain Nation States", Institute for Security Technology Studies, Dartmouth University, 2004, p. 4.

## Portugal

Portugal does not have a cybersecurity strategy, but its "Knowledge Society Agency" is tasked with developing one. Portuguese cyber legislation covers a wide range of computer-related fraud and exploitation, expanding upon the recommendations of the European Council. The Portuguese Judicial Police force includes a unit specialized in cyber and information-related crime, known as the Central Investigations Section for IT and Telecommunications.[226]

## The Philippines

The Task Force for the Security of Critical Infrastructure first issued the National Cyber Security Plan in 2005. The strategy involves reducing cyberspace vulnerabilities under the Philippine jurisdiction, nurturing a culture of cybersecurity among individual users and critical sectors, and strengthening self-reliance on IT technology and human resources.[227] The Task Force also created the Government Computer Security Incident Response Team, tasked with detecting and investigating computer network intrusions and incidents.[228]

The National Cyber Security Office implements national cybersecurity policy, in charge of implementing measures to prevent, suppress and investigate cybercrime, and coordinate with the private sector, local governments, non-governmental organizations and international partners in enhancing cybersecurity. It is part of the Commission on Information and Communications Technology, the primary administrative agency in the Philippines government that promotes, develops, and regulates the national information and computer technology infrastructure.[229]

## 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.[230] Serbia opened its Cyber Crime Department in 2005, which specializes in cybercrime court cases. It became operational in 2007, overseeing the judicial process for cybercrime prosecution throughout the country.[231] Serbia's Republic Agency for Telecommunications is playing a leadership role in Internet regulations and information security issues, and the agency passed legislation in 2008 on "Instructions for Technical Requirements for Subsystems, Devices, Hardware and Installation of Internet Networks".

---

226 "Portugal Country Report", European Network and Information Security Agency, 2010, <www.enisa.europa.eu/act/sr/files/country-reports/Portugal.pdf>, pp. 5–8, 22.

227 "Philippine Cybersecurity Efforts", National Cybersecurity Coordination Office, <www.itu.int/ITU-D/asp/CMS/Events/2010/NGN-Philippines/S5-Philippines_cybersecurity.pdf>, p. 44.

228 Roy Sinfuego, "Government cyber watchdog launched", *Manila Bulletin,* 9 August 2004.

229 Both of the following presentations are similar, although the latter describes the tasks of the National Coordinator for Cybersecurity in more detail; "Philippine Cybersecurity Efforts", Philippine National Cybersecurity Coordination Office, <www.itu.int/ITU-D/asp/CMS/Events/2010/NGN-Philippines/S5-Philippines_cybersecurity.pdf>; Virtus V. Gil, "National Cybersecurity Efforts", <www.isssp.org.ph/afpsummit-031010/AFPSummit-National%20Cyber%20Security%20Efforts-Gil.pdf>.

230 *National Security Strategy of the Republic of Serbia*, 2009.

231 "Courtrooms of cyber-crime department opened", Government of Serbia, 12 April 2007.

This legislation set the privacy and security standards for Internet service providers and producers of hardware and software.[232]

## Singapore

Singapore's cyber policy focuses on the security of information technology and the telecommunications industry. The Singapore Infocomm Technology Security Authority oversees all operational IT security and protects Singapore from threats at the national level. This agency operates under the Internal Security Department of Singapore's Ministry of Home Affairs.[233] The Authority has a programme to enlist individual IT professionals to serve as cyber defenders.[234]

The National Infocomm Security Committee formulates cyber policy and security strategy. The committee is under the purview of the Singapore Infocomm Development Authority. It issued in 2005 the Infocomm Security Masterplan, which details the multi-agency efforts to ensure cybersecurity.[235] This policy is led by the Infocomm Development Agency, and is designed to provide security to the population and to the private and public sectors by raising awareness about cyber risks and developing appropriate security measures. It also will develop national capabilities, enhance security technology research and development, and improve critical infrastructure resilience.[236] This entails the creation of a National Cyber-Threat Monitoring Centre.[237]

## Slovakia

Slovakia's National Strategy for Information Security established a security framework for critical infrastructure and emphasizes deterring attacks, building defence, and maintaining sustainable infrastructure.[238] Slovakia's 2010 Government Security Plan cites a rise in recent cyberattacks as cause for concern and a catalyst to increase cyberdefences. The government seeks to engage with allies to build domestic capacity. Slovakia is also a member of the NATO Cooperative Cyber Defence Centre of Excellence.[239] Slovakia has also signed agreements with NATO to cooperate in the event of a cyberattack and is assisting with the development of guidelines for practical cyber cooperation among NATO partners.[240]

232 "Serbian telecom agency publishes internet traffic interception laws", *European Digital Rights*, 30 July 2008.

233 Sumner Lemon, "Singapore to form national cyber security agency", *IDG News*, 30 September 2009; Wendell Minnick, "Singapore beefs up cyber security", *DefenseNews*, 5 October 2009.

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

235 For the most recent Masterplan, see *InfoComm Security Masterplan 2*, Singapore Infocomm Development Agency, 5 April 2010.

236 Ibid.

237 "Singapore gears up for cyber security", Infocomm Development Agency, 22 February 2005.

238 "Slovakia Country Report", European Network and Information Security Agency, 2011, <http://www.enisa.europa.eu/act/sr/country-reports>, pp. 5–6.

239 "NATO opens new centre of excellence on cyber defence", *NATO News*, 14 May 2008.

240 Jeffrey Hunker, "Cyber War and Cyber Power: Issues for NATO Doctrine", Research Paper no. 62, NATO Defense College, 2010, pp. 8–9.

## Slovenia

Slovenia sees the cyber domain as a new area of warfare and will establish public–private partnerships and a national coordinating body. Slovenia's National Security Strategy emphasizes the dangers of cyber risks and the misuse of information technologies as a significant transnational risk to national security.[241] In the future, this risk will shape the objectives of international warfare, in that the goal will be to destroy enemy capabilities with non-traditional cyber means. The army acknowledges the electromagnetic spectrum as one of the five dimensions of future war.[242]

Slovenia will create a national strategy to respond to these threats that will emphasize domestic measures. It will engage the private sector to help with this effort. One of the tasks will be to create a national cyber coordination body that will manage these defences for various government agencies. One aspect of their cyber strategy will focus on fighting the dissemination of "illegal content" on the web.[243]

## South Africa

The South African Cabinet and the Ministry of Communication are drafting a cybersecurity policy that will be considered in 2011. It will call for the establishment of a Cyber Inspectorate, which will become operational in 2012.[244]

South African cybersecurity policy has the following objectives: establish relevant structures, reduce threats, facilitate cooperation between government agencies, and build capacity. The National Cybersecurity Advisory Council will coordinate cybersecurity policy. The Council will advise the Minister of Communication, ensure cooperation between government agencies, encourage public–private partnerships, provide current threat assessments, and implement cyber policy.[245]

## Spain

Royal Decree 3/2010 adapted Spain's 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 multi-layered "defence in depth" strategies, and that security will include measures of prevention, detection and mitigation.[246] Although it does not lay out principles for pre-emptive or retaliatory action beyond national borders, preventive measures are stated to include not only lessening exposure to potential threats but also dissuasion.[247] The

241 *Resolution on the National Security Strategy of the Republic of Slovenia*, Slovenian Ministry of Defence, 2010, pp. 14, 16-17.

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

243 *Resolution on the National Security Strategy of the Republic of Slovenia*, Slovenian Ministry of Defence, 2010, p. 38.

244 *Strategic Plan 2010–2013*, South African Department of Communications, <www.info.gov.za/view/DownloadFileAction?id=144185>, p. 23.

245 *Draft Cybersecurity Strategy of South Africa*, 19 February 2010, <www.pmg.org.za/files/docs/100219cybersecurity.pdf>, pp. 4–5.

246 *National Security Framework*, Government of Spain, 2010, <www.csi.map.es/csi/pg5e42.htm>.

247 Enrique Fojon Chamorro and Angel F. Sanz Villalba, "Cyber Security in Spain: A Proposal for its Management", Real Instituto Elcano, 29 July 2010; *Spanish National Security Framework*, Royal Decree

National Cryptology Center of the National Intelligence Centre is the body responsible for the security of government networks and classified national security information and manages the government's computer emergency response team.[248]

## Sweden

Sweden is creating policies and institutions to defend against cyber threats. Sweden's Civil Contingencies Agency (MSB) will set up a national operational coordination centre for cybersecurity.[249] This centre will focus on preventative work and coordinate incident response. It will also work closely with the Swedish Armed Forces to analyze future systems to protect confidential information.[250] In 2011, Sweden released a "National Response Plan for Serious IT Incidents" that emphasized cooperative approaches with industry and other agencies to minimizing disruption.

## The United Arab Emirates

The United Arab Emirates is launching a cyber operations centre. The first phase of the United Arab Emirates Command and Control System was completed in February 2011. The centre is a joint effort between the firm Emiraje Systems and Khalifa University and will coordinate with the armed forces.[251] The state has a computer emergency response team, established by the Telecommunications Regulatory Authority in 2008. It currently serves as the state's cybersecurity coordination centre.[252]

## Viet Nam

Viet Nam's General Department of Logistics and Technology–Ministry of Public Security, the Viet Nam Computer Emergency Response Team, and International Data Group continue to draft plans for information security advancements throughout the next decade.[253] Viet Nam is planning to invest $42 million to secure sensitive information and establish a National Centre for Technology and an Agency for Information Security.[254]

## Zimbabwe

Zimbabwe is developing policies and capabilities to ensure cyber security. According to the 2010–2014 Strategic Plan by the Ministry of Information Communication Technology (MICT), Zimbabwe would create a Cyber policy in 2010,[255] which would be implemented and monitored by MICT through 2013.[256]

---

3/2010, 8 January 2010.

248 Ibid.

249 "Measures to improve Sweden's ability to prevent and handle IT incidents", Swedish Civil Contingencies Agency, 13 January 2010.

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

251 Matthew Bell, "Cassidian completes first phase of UAE cyber centre", *Jane's*, 24 February 2011.

252 "UAE Region signs MoU with CERT to reinforce information security", *DP World*, 12 April 2011.

253 "Press Release Security World 2011", Security World 2011 Conference and Expo, 3 March 2011, <www.citek.com.vn/newsdetail.php?id=380&cat_id=1037>.

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

255 It is unclear if this policy has been created.

256 Strategic Plan 2010–2014, Ministry of Information Communication Technology, <www.techzim.co.zw/wp-content/uploads/2010/02/zimbabwe_mict_strategic_plan2010-2014.pdf>, pp. 22–24.

UNIDIR RESOURCES

## About UNIDIR

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.