RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE STUDIES

Background Paper

Military Cyber Defense Structures of NATO Members: An Overview

Matteo Gramaglia (Visiting Research Fellow)

Emmet Tuohy (Research Fellow)

Piret Pernik (Research Fellow)

December 2013

Summary

The aim of this report is to give an overview of the institutions and structures through which NATO member militaries handle cyber defense (CD); examples include cyber commands, military CERTs/CIRCs, special cyber units, and so on. As anticipated, open-source information on the development of military CD capabilities is scarce and relatively general in nature. Nevertheless, after a thorough review of existing public sources (which are listed by state in the appendix), we have been able to identify some tentative findings of interest, as found in the conclusions.

To date 14 of the 28 NATO member states have established special military cyber defense units: Canada, Denmark, Estonia, France, Germany, Greece, Italy, Latvia, the Netherlands, Norway, Poland, Turkey, the United Kingdom, and the United States. These units vary from rudimental capability such as a very small military unit or CIRC to mature capability such as a full-fledged Cyber Command. Only very few states have formed a Cyber Command. Five other NATO states are either in the process of developing or have firm plans to develop military CD capabilities, often including the establishment of a special unit: Albania, Bulgaria, Portugal, Lithuania, and Luxembourg. Thus, a clear majority (19) of allied militaries have taken constructive action on military cyber defense.

Further research is necessary in order to determine whether existing open-source information is sufficient to permit meaningful description and comparative analysis of the duties, objectives, and responsibilities of these units.

COUNTRY REVIEW

ALBANIA

While Albania has not yet released any unified national cyber security (CS) strategy, its military has undertaken several different initiatives to enhance cyber defense. For example, in 2010 the Ministry of Defense assigned responsibility for developing CD capability to the newly-created Inter-Institutional Maritime Operation Center. Its Department of Research and Technological Development is responsible for developing new solutions for cyber threats. In its 2013 Defense Directive, the ministry gave new momentum to the capability-building process by stressing the necessity of creating new elements of CD within the country, such as a national CERT.

BELGIUM

Belgium has made relatively little progress towards developing CD capabilities. Even in civilian terms, the country lags behind its allies—it has no CS strategy, with responsibilities for CD spread across various government agencies. That said, some of these institutions have recently been advocating for greater security measures, and some concrete steps have been taken, particularly in terms of critical infrastructure (CI). Particularly relevant is the role of the Belgian Network Information Security platform, which advises other government agencies on cyber threats and CI protection. Belgium has also recently signed a memorandum of understanding with the Netherlands and Luxembourg regarding cooperation on cyber security.

BULGARIA

Information on military CD in Bulgaria is rather scant. In a 2010 white paper, Bulgaria's Ministry of Defense stated that it was working towards building a single information network, acknowledging the necessity of strengthening cyber defense for this purpose. Recently, the ministry announced that it is now planning to establish a CD unit within the Armed Forces Reserve. The country has yet to adopt a CS strategy but has created an Incident Response Team, while also declaring its intention to establish a National Cyber Security Authority in order to enhance defense capabilities while implementing training programs. However, close cooperation with both NATO and the EU is considered fundamental for Bulgaria to finalize its national CS strategy and other key documents.

CANADA

In the Canadian Forces (legally separate from the Department of National Defence), there is a specific Information Management group tasked with protecting communications and computer networks. In June 2011, the Canadian Forces Chief of Force Development announced the establishment of a new organization, the Directorate of Cybernetics, to build cyberwarfare capabilities for the armed forces.

Canada adopted its CS strategy in 2010, focusing mainly on securing government systems and public network. Public Safety Canada, the federal government department [ministry] responsible for homeland security, oversees implementation of the strategy. The Canadian Security Intelligence Service, also responsible to the minister for public safety, has some responsibility for information security threats. Some CS functions remain under the umbrella of the Department of National Defence, however, specifically its Communications Security Establishment, which operates the Government of Canada Cyber Threat Evaluation Centre.

CROATIA

Open-source information on CS and CD in Croatia is minimal. It appears that the internet security of the government's own systems is handled by the Security and Intelligence Agency, although it seems to concern itself primarily with data protection. That said, Croatia has held numerous meetings with NATO to define the future CS and CD challenges for the country in terms of cyber security, particularly the role the Alliance can play in strengthening the capabilities of the Croatian Defense Forces.

CZECH REPUBLIC

The Czech Republic has yet to produce a CS strategy as such. However, it is in the process of development in the Ministry of Interior, which coordinates cyber security issues and which has a department dedicated to Cyber and Informational Security. CI was a particular focus of the National Security Research Strategy approved in 2008, while in 2010 the country formally established a CSIRT.

DENMARK

With the release of the new of the Danish Defense Agreement 2013-2017, Denmark moved from the primarily defensive CD approach seen in the previous document to a more balanced one. The country's priorities have not changed, however, and remain the protection of military computer systems and other IT infrastructure. Both a governmental and a military Centre for Cyber Security (GOvCERT) have been established. Finally, the Defence Intelligence Service is responsible for finding and countering cyber threats.

FRANCE

In the field of CD, both the army and navy have both CERTs and declared cyber attack capabilities. Furthermore, there is an intelligence agency within the Ministry of Defense called the Directorate for Defence Protection and Security, which seeks to maintain the military's operational capacity by providing information about potential threats and vulnerabilities. France also has specifically remarkable capabilities in cryptology, a principal area of cyber defense. The Network and Information Security Agency operating under the Ministry of the Interior plays the main coordinating role within the French CS framework, which is set forth in two main documents: the White Book (2013) and the Strategy on Information Systems.

GERMANY

In terms of military CD in Germany, Department of Information and Computer Network Operations of the armed forces' Strategic Reconnaissance Unit is tasked with developing cyber capabilities. As for CS, the country published its strategy in 2011 under the supervision of the Ministry of Interior, which also established a National Cyber Response Center at that time. The Center incorporates officials from the Federal Criminal Police Office, the Federal Police, the Customs Criminological Office, the Federal Intelligence Service, critical infrastructure regulators, and importantly, the armed forces. There is also a National CS Council that focuses on major attack prevention and counter measures, including all relevant ministries and relevant private actors; it is responsible for coordinating defense techniques and cyber policy.

GREECE

Despite having no civilian CS strategy as of yet, Greece has a comparatively long history in CD, establishing its military Office of Computer Warfare in 1999. This office was followed by the creation of the Directorate of Cyber Defense under the ChoD in 2011. The Directorate is responsible for defending against acts of cyber warfare and to this end coordinates with the National Intelligence Service (NIS) and the police. Under the NIS, in 2008 Greece established a CERT (the National Authority against Electronic Attack), which shares responsibilities with other CERTs from the private and university sectors.

HUNGARY

In Hungary, the Ministry of Defense is responsible for information security and has developed special classes at the Zrinyi Defense Academy to develop military cyber security capabilities. The country has yet to produce a CS strategy, though the 2012 National Security Strategy identifies the need to ensure the operation of critical infrastructure networks, assess and prioritize cyber risks, raise public awareness of cyber threats, and work with international partners to protect secure information systems. There is a National Cyber Security Center, part of the Prime Minister’s Office and led by the latter’s Information Security Supervisor, tasked with protecting central government systems as well as critical infrastructure from cyber attack; it also hosts the country’s CERT.

ICELAND

To date, in Iceland cyber security responsibilities have been informally divided among the Ministry of the Interior, the Post and Telecom Administration, the Icelandic Police, and the Data Protection Authority. The Ministry of the Interior is now formally developing a national CS strategy, however. Last year, a national CERT was activated, and seems to be partly operational.

ITALY

The Italian military has an electronic warfare unit responsible for intelligence, surveillance, target acquisition, and reconnaissance. Other military CD establishments include Defense Innovation Centre and the Division for Information Security of the Defense Staff. Additionally, the Telematics Department of the Carabinieri [military police] General Staff has been established to combat cybercrime and terrorism.

While Italy has yet to publish a formal CS strategy, it is likely to do so soon. Moreover, many initiatives have already been enacted. For example, last January a law that determines roles and responsibilities regarding cyber security was approved. At the top of the decision-making process is the Committee for Security of the Republic (CISR) composed by the prime minister and the Council of

Ministers, which will assess the implementation of the forthcoming strategy. This Committee is supported by the Department of Information for Security (DIS), which hosts the Italian CIRC. The law also provides for the creation of a CERT coordinated by the military advisor to the Prime Minister.

LATVIA

Latvia currently has no national CS strategy, but CS issues remain of paramount importance to the Latvian government at all levels. Its 2012 National Security Concept and State Defense Concept prioritize CI protection in particular. The Information Technology Security Act (legislation that has been in force since 2011) requires every state agency in Latvia to appoint a Head of Security for information technology to ensure that data is kept safe in case of emergency or natural disaster. A government-established CERT/CSIRT—under the Ministry of Defense—carries out monitoring, risk assessment, recommendations, incident handling &assistance, awareness raising, exercises, and research functions.

LITHUANIA

Lithuania published its CS strategy in 2011 (the Program for the Development of Electronic Information Security) which establishes priorities and responsibilities for CS and CD. The Program also sets a 2015 deadline for the creation of a Cyber Defense Plan to address the critical information infrastructure of defense institutions, to be followed by a National Cyber Defense Plan in 2019, covering national critical information infrastructure and information resources. A national CERT has been established and its responsibilities have been clarified in legislation, entitled “Approval of the Rules on Ensuring the Security and Integrity of Public Communications Networks and Public Electronic Communications Services.” Lithuania also works closely with Estonia and Latvia on CS areas of interest.

LUXEMBOURG

Luxembourg has had a CS strategy since 2003, a document that was renewed in 2011. Given Luxembourg’s role as a major banking and financial center, the institution in charge of developing the strategy was the Ministry of the Economy and Foreign Trade, and the main focus points were cybercrime and partnerships between the public and private sector. A CERT/CSIRT was established in 2001 under the Council of State.

NETHERLANDS

The Netherlands has an exceptionally well-developed approach to CD and CS. Its cyber security strategy, released in 2012, was published by the Ministry of Defense. The strategy also includes a conceptualization of offensive measures. That same year, the Dutch government also created a National Cyber Security Center replacing the previous GOVECERT. In its short history to date, the Center has already published two key documents: a security checklist for supervisory control & data acquisition for industrial control systems, and the Cyber Security Assessment Netherlands report, which assesses the short-term goals and needs of the government regarding cyber security. In its coordination role, the Center is directed by the Ministry of Interior with strong collaboration from the Ministry of Defense. In January 2012, the military established Defense Taskforce Cyber in order to gather intelligence on cyber activities and threats, as well as to create closer coordination with the Cyber Unit. The National Coordinator for Counter-Terrorism has also expanded its mission to include a cyber component, specifically in testing the vulnerability of internet applications against cyber attack.

NORWAY

In September 2012, the Norwegian Armed Forces established the Cyber Defense Force as a ”separate entity tasked with securing the Armed Forces against cyber threats.” The CDF also includes the Centre of Excellence for Command, Control and Information Systems. On the civilian side, Norway also published its CS strategy in 2012, a document that underlines the roles and responsibilities of different stakeholders. One particularly relevant stakeholder is the National Security Authority, which includes the national CERT; it is jointly supervised by the Ministry of Defense and the Ministry of Justice.

POLAND

Responsibility for CS in Poland is divided between the Ministry of Administration and Digitization and the Internal Security Service. The Ministry of National Defense also has significant cyber responsibilities for military networks. In 2010, Poland developed the Governmental Action Plan for Cyber Security 2011–2016. It called for the creation of an Interministerial Coordination Team for Protection of Cyberspace that would include a new post of Government Representative for Protection of Cyberspace as well as representatives from other public and private entities. The Ministry of Administration and Digitization now has responsibility and has set up a task force for implementation. The government CERT, managed by the Internal Security Service, has responsibilities for both public and private networks, including critical infrastructure. The Computer Incident Response System is responsible for cyber security in the Ministry of National Defense. The System is supervised by the Director of the Information Technology and Telecommunication Department, who coordinates cyber security functions and is supported by the Ministerial Centre for Network Security and ICT Services Management.

PORTUGAL

Within Portugal’s armed forces, a Cyber Defense Team has been established and is developing operational features. On the whole, without any official CS strategy as such, Portugal seems to be focused primarily on criminal threats in cyberspace. The most relevant actors are the Judicial Police (with its Central Investigation Section for IT and Telecommunications) and the Ministry for Home Affairs. In addition, the Security Intelligence service also focuses overwhelmingly on crime. That said, Portuguese legislation on other cyber issues, particularly CI protection, is quite advanced.

ROMANIA

Romania's National Security Strategy mentions cyber terrorism, but the country does not have a CS strategy at the moment. Nonetheless, several different institutions have been created to enhance cyber security. The Service for Countering Cyber Criminality, part of the Directorate for Countering Organized Crime, is responsible for preventing and investigating cyber attacks, while the national CERT serves as a hub for information security and promoting awareness of potential cyber threats.

SLOVAKIA

In terms of CD, The Defense Strategy of the Slovak Republic recognizes cyber threats as a "game changer" for the security environment. The country has yet to produce a CS strategy, but cyber security is pursued widely, through various agencies belonging to different ministries. Coordination is overseen by the National Security Agency through an inter-ministerial working group. Meanwhile, a government CSIRT has been founded under the Ministry of Finance.

SLOVENIA

Although Slovenia does not have a civilian CS strategy, its National Security Strategy emphasizes the dangers of cyber threats and the misuse of information technologies as significant risks to national security. The military also considers cyber threats relevant, declaring cyber warfare as one of the five dimensions it sees of future war.

SPAIN

The main player in Spanish CD is the Ministry of the Interior, which coordinates the relevant operations of the Armed Forces. The National Intelligence Centre is responsible for the security of government networks and classified national security information and manages the government's CERT (established in 2006). The country also has two separate cyber police forces. Spain adopted a CS strategy in 2011.

TURKEY

CD has become a focus for the Turkish military, which recently established a Cyber Army Command subordinated to the General Staff. On the civilian side, the government has set up a Cyber Security Board, which in collaboration with other government bodies is now preparing a CS strategy. This effort has been given new impetus by the Syrian crisis and the corresponding rise in the risk of a cyber attack.

UNITED KINDOM

The United Kingdom has a wide and advanced concept of cyber security. Its 2011 CS strategy remains to day one of the most comprehensive ever published, covering both nation-state attacks and cybercrime. The Office of Cyber Security and Information Assurance, created in 2009, provide strategic direction and coordinates cyber security policy from within the Cabinet Office. Also relevant to CS is the Centre for the Protection of National Infrastructure. Last but not least, there are two main Cyber Centres for Defence, one in the Home Office [ministry of internal affairs] and one in the Ministry of Defence.

UNITED STATES

Under President Obama, the US military has significantly strengthened and expanded its role in cyber defense. US Cyber Command established in 2010 and originally responsible for dealing with threats only to the military's own cyber infrastructure, has recently been given broader national CD responsibilities, which include both defensive and offensive operations.

In terms of defining and understanding cyber security, the US has long been a world leader. It has published several CS strategies already. Responsibility for cyber security is divided among several Cabinet departments [ministries]—including the Department of Homeland Security, the Federal Bureau of Investigation (part of the Department of Justice), and the Department of Defense, including US Cyber Command (which in turn has the National Security Agency as one of its component parts). 13 federal agencies participate in the National Cyber Response Coordination Group, which is responsible for coordinating the federal response among them in the event of a ”nationally significant cyber incident.”

Tentative Conclusions

Considering the increasing complexity and scale of cyber challenges as well as the broad scope of NATO as an organization, on the whole the efforts of the Alliance and its members to increase their cyber defense and cyber security capability must be judged positively. However, even from our brief portrait it is quite apparent that the main theme is the variety of different approaches that NATO and member countries have taken to the subject.

Accordingly, the first recommendation to emerge from this report is that NATO will continue to advocate for a clear understanding of cyber defense and cyber security threats, something that in time could become a shared understanding of cyber concepts. From this basis, the Alliance could more easily ensure information sharing not just between NATO headquarters and member states, but among the member states themselves.

As the threats from cyberspace are no longer new, a cyber revolution is not needed; what is required instead is an evolution of existing management in this sphere. Best practices among existing states should be highlighted, joint operations enhanced, and awareness campaigns carried out. Specifically, considering the lingering effects of the economic crisis and the limited means of many current governments, NATO should continue to exploit more fully the possibilities raised by the smart defense concept, emphasizing the capacities and abilities of some of members, whether Estonia in public-private partnerships, France in cryptology, or Luxembourg in financial networks, in order to expand these capacities to other members.

In the end, NATO has already undertaken major changes in the way it confronts cyber threats. The process of enhancing security is a long-term one, although many steps can be made also in the present. Particularly in the nine states still lacking in formal military cyber defense structures, the main challenge is to create effective agencies with a comprehensive legal mandate for enacting and implementing reforms as quickly as possible.

Moreover, it is time for NATO itself to work more actively to facilitate increased cyber security among its members. As a first step, it should establish high common standards, while being ready to provide assistance to states that encounter difficulties in implementing them. Subsequently, the Alliance should spark moves towards more specialized cyber defense capabilities (e.g., by training more cyber experts) and towards more concrete capabilities in specific areas (e.g., in cloud computing), always keeping in mind the principle of smart defense.

APPENDIX: Sources by Country

Albania

http://www.mod.gov.al/eng/images/defensedirective.pdf

http://www.mod.gov.al/eng/index.php?option=com_content&view=article&id=2078:ncsd&catid=350:ncsd&Itemid=681

http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Belgium

http://www.mil.be/def/doc/index.asp?LAN=fr&ID=355

https://www.cert.be/pro/

http://suretedeletat.belgium.be/fr/

http://www.comiteri.be/index.php?option=com_content&task=view&id=53&Itemid=152&lang=FR

http://diplomatie.belgium.be/search?language=en&search_field=cyber&search_submit=search

http://www.lachambre.be/doc/ccri/pdf/53/ic750.pdf#search="cyber command"

Bulgaria

http://news.xinhuanet.com/english2010/world/2011-10/19/c_131201077.htm

http://www.mod.bg/en/doc/misc/20101130_WP_EN.pdf

http://www.md.government.bg/en/doc/programi/20130325_prioriteti_MoD.pdf

http://www.md.government.bg/en/doc/drugi/20120620_Doklad_2011.pdf

Canada

http://www.publicsafety.gc.ca/index-eng.aspx

http://www.cse-cst.gc.ca/gtec/speech-2013-10-09-eng.html

Croatia

http://www.cert.hr/en/start

http://www.morh.hr/en/pretraga.html?searchword=cyber&searchphrase=all

http://www.morh.hr/en/news/press-releases/8109-nato-defence-ministerial-concluded.html

https://www.soa.hr/en/soa/scope/

Czech Republic

http://www.cybersecurity.cz/main_en.html

https://www.csirt.cz/

http://www.govcert.cz/en/

Denmark

http://www.fmn.dk/Eng/Pages/Frontpage.aspx

http://www.fmn.dk/nyheder/Documents/danish-defence-agreement-2010-2014-english.pdf

http://www.fmn.dk/eng/allabout/Pages/DanishDefenceAgreement2013-2017.aspx

http://www2.forsvaret.dk/Pages/sogning.aspx?k=cyber&u=http://www2.forsvaret.dk

http://www.forsvaret.dk/TGR/Pages/sogning.aspx?k=cyber&u=http://forsvaret.dk/tgrhttp://fe-ddis.dk/cfcs/opgaver/govcert/Pages/default.aspx

http://www.govcert.cz/en/

France

http://www.ssi.gouv.fr/fr/defense-des-si/

http://www.defense.gouv.fr/dpsd/la-dpsd/un-service-de-renseignement/un-service-de-renseignement

http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf

http://www.defense.gouv.fr/portail-defense/rubriques-complementaires/recherche?SearchText=cyber&subtree=2

Germany

http://www.bmi.bund.de/EN/Topics/IT-Internet-Policy/it-internet-policy_node.html

https://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Germany.pdf

http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

Greece

http://www.nis.gr/portal/page/portal/NIS

http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Greece.pdf

http://www.onalert.gr/stories/Antimetopish_kybernoepitheseon_sto_GEETHA

http://cert.grnet.gr/

http://www.mod.mil.gr/mod/en/content/show/46/342

http://www.geetha.mil.gr/index.asp?a_id=3461&nid=3112

http://www.cert.auth.gr/index.php/el/

http://www.infosoc.gr/infosoc/en-UK/default.htm

Hungary

http://www.cert-hungary.hu/en/node/7

http://www.kormany.hu/en/search#category=all&search=cyber

http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Hungary.pdf

http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Iceland

http://www.cert.is/

http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Iceland.pdf

http://www.personuvernd.is/information-in-english/

http://eng.forsaetisraduneyti.is/information-society/English/nr/1248

http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Italy

http://www.sicurezzanazionale.gov.it/sisr.nsf/il-mondo-intelligence/principi-strategici-delle-politiche-di-cyber-security.html

http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Italy.pdf

http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg;jsessionid=QI0W7ckcZt5e7NUAX7Rj3Q__.ntc-as1-guri2a

http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Italy.pdf

http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Latvia

http://www.mod.gov.lv/

http://www.mil.lv/lv/Aktualitates/Tavai_drosibai.aspx

http://cert.nic.lv/

http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Lithuania

http://www.ird.lt/doc/teises_aktai_en/EIS(KS)PP_796_2011-06-29_EN_PATAIS.pdf

https://www.cert.lt/

http://www.lrvk.lt/bylos/vyriausybes/en_15_programa.pdf

http://kariuomene.kam.lt/en/search/results.html

http://www.kam.lt/en/search/results.html

http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Luxembourg

http://www.gouvernement.lu/2811947/BID_2_2012

http://www.govcert.lu/en/

https://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Luxembourg.pdf

http://www.restena.lu/restena/en/EN-Index.html

Netherlands

https://www.ncsc.nl/english/

https://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011

http://www.rijksoverheid.nl/zoeken?keyword=cyber&search-submit=Zoek

http://www.defensie.nl/servicemenu/zoeken/?query=cyber

Norway

http://www.regjeringen.no/en/dep/fad/documents/Reports-and-plans/Plans/2012/cyber-security-strategy-for-norway.html?id=710469

http://www.regjeringen.no/upload/FD/Dokumenter/Fakta-om-Forsvaret-2013_engelsk_oppdatert-mai-2013.pdf#search=cyber

http://forsvaret.no/OM-FORSVARET/ORGANISASJON/CYBERFORSVARET/Sider/cyberforsvaret.aspx

https://www.nsm.stat.no/Engelsk-start-side/

Poland

http://www.abw.gov.pl/pl

http://www.cert.gov.pl/cee/arakis-gov-system/78,ARAKIS-GOV-system.html

http://www.archiwalny.mon.gov.pl/pliki/File/vision_of_paf_2030.pdf

https://mac.gov.pl/wp-content/uploads/2013/06/Polityka-Ochrony-Cyberprzestrzeni-RP_wersja-ang.pdf

http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Poland.pdf

http://archiwalny.mon.gov.pl/en/wyszukaj/

Portugal

http://www.sis.pt/ciberameaca.html

https://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Portugal.pdf

http://www.exercito.pt/Search/Results.aspx?k=ciber

Romania

http://www.cert-ro.eu/?lang=en

http://www.efrauda.ro/pages.do?lang=en&idMenu=1

http://www.mapn.ro/smg/#

Slovakia

http://www.nbusr.sk/en/

http://www.csirt.gov.sk/

http://www.mod.gov.sk/vysledky-vyhladavania/?search=cyber&amp;x=-1099&amp;y=-60

Slovenia

http://elivinglab.org/Government/

http://www.mo.gov.si/en/search/

http://elivinglab.org/CrossBordereRegion/DeRc/Presentations/Kastelic_CyberSecurity.pdf

http://www.slovenskavojska.si/iskanje/

http://www.slovenskavojska.si/fileadmin/slovenska_vojska/pdf/vojaski_izzivi/svi_13_3.pdf

Spain

https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=12&Itemid=32&lang=en

http://www.cnpic-es.es/Ciberseguridad/index.html

http://bit.ly/1hOLXYT

http://www.cni.es/en/welcometocni/

http://bit.ly/1fr8H0I

http://www.defensa.gob.es/

http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Spain.pdf

Turkey

http://www.trdefence.com/2010/09/09/turkey-creates-its-own-nsa/

http://www.tubitak.gov.tr/en

http://www.turkishnews.com/en/content/2011/10/04/turkey-establishes-the-national-cyber-security-coordination-foundation/

http://www.aa.com.tr/en/news/124195--turkish-armys-new-cyber-defense-unit

http://www.tsk.tr/ing/

United Kingdom

https://www.gov.uk/government/policy-teams/128

http://www.cpni.gov.uk/

https://www.gov.uk/search?q=cybersecurity&tab=government-results

United States

http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

http://www.dhs.gov/topic/cybersecurity

http://www.dhs.gov/office-cybersecurity-and-communications

http://www.defense.gov/home/features/2010/0410_cybersec/index.html

http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf

http://www.jcs.mil/page.aspx?id=2

http://www.state.gov/s/cyberissues/index.htm