P|I|P|S Brief No. 4.4

MAKING THE GRADE
AN INTERNATIONAL REGULATORY FRAMEWORK FOR CYBERSECURITY

Emily Pehrsson

The Project on International Peace and Security
The College of William and Mary

The Project on International Peace and Security (PIPS) at the College of William and Mary is a highly selective undergraduate think tank designed to bridge the gap between the academic and policy communities in the area of undergraduate education. The goal of PIPS is to demonstrate that elite students, working with faculty and members of the policy community, can make a meaningful contribution to policy debates. The following brief is a testament to that mission and the talent and creativity of William and Mary's undergraduates.

Amy Oakes, Director
Dennis A. Smith, Director

The Project on International Peace and Security
The Institute for Theory and Practice of International Relations
Department of Government
The College of William and Mary
P.O. Box 8795
Williamsburg, VA 23187-8795
757.221.5086
pips@wm.edu

MAKING THE GRADE:
INTERNATIONAL REGULATORY FRAMEWORK FOR CYBERSECURITY

EMILY PEHRSSON

Vulnerable states, defined as states unable or unwilling to crack down on cyber crime within their borders, threaten U.S. cybersecurity. Current U.S. policy offers technology transfers to like-minded states to secure their cyber networks, without requiring these states to make cybersecurity a domestic policy priority. This brief proposes a voluntary, private-sector based cybersecurity grading system paired with security incentives administered through NATO to encourage improvements in cybersecurity. Participating states will be awarded grades based on the quality of their cybersecurity infrastructure. Incentives will increase incrementally with each security grade attained and include access to: (1) law enforcement training programs; (2) NATO cyber rapid reaction teams; (3) limited technology transfer; and (4) intelligence sharing. The proposed framework would initially apply to NATO members and would later be expanded to select non-member states. The grades framework and incentives will act as a short- to medium-term incentive for the rapid development of international cybersecurity standards and reduce long-term costs for the United States.

Strategic Importance of Cybersecurity

Increasing government, military, and industry reliance on the cyber domain has incentivized cyber crime and heightened the cost of internet disruptions. In 2010, cyber attacks rose 93% worldwide with approximately 55,000 pieces of malware introduced daily.[1] In 2011, U.S. authorities shut down a cyber botnet that stole $97 million and hijacked over 2 million computers, the majority of which were located in the United States.[2] The frequency and sophistication of cyber attacks will continue to rise as access to computers increases worldwide.[3]

Dangers of U.S. Cyber Insecurity

In 2010, the U.S. Computer Emergency Readiness Team (US-CERT) received 41,776 reports of malicious cyber incidents in federal networks, an increase of 39% since 2009.[4] Cyber attacks can threaten U.S. military operations, national critical infrastructure, information security, and economic competitiveness through:

- *Military Network Vulnerability*: From November 2008 to April 2009, the Pentagon spent approximately $100 million repairing damage from and addressing the

repercussions of cyber attacks.[5] Unauthorized users probe Department of Defense networks about 250,000 times every hour and over 6 million times per day.[6]

- *National Critical Infrastructure Vulnerability:* The U.S. Cyber Command only protects .mil domains, leaving the largely civilian-owned national critical infrastructure more vulnerable to attack. McAfee estimates that a major cyber crime attack would cost each company in the oil and gas sector approximately $8.4 million per day.[7] Deputy Defense Secretary William J. Lynn stated: "It is possible to imagine attacks on military networks or on critical infrastructure like the transportation system and energy sector that cause severe economic damage, physical destruction or even loss of life."[8]

- *Cost of Intellectual Property Theft*: McAfee estimates that intellectual property and proprietary information theft costs approximately $1 trillion annually.[9] The FBI stated that the cost to the United States equals about $400 billion every year.[10] Cyber criminals disproportionately target the United States. For example, Operation Shady RAT compromised the networks of over 71 organizations, two-thirds of which were in the United States.[11] A study released in 2010 by the Ponemon Institute estimated that each victim organization bears a median yearly cost between $1 million and $52 million as a result of cyber crime.[12]

Cyber Threats from Vulnerable States

Vulnerable states such as Romania, Bulgaria, and Slovenia are less willing and able to devote significant government resources to locating and extraditing cyber criminals and dismantling organized cyber crime groups, allowing these groups to threaten U.S. cybersecurity. A 2011 National Security Council report stated that "through cyber crime, transnational criminal organizations pose a significant threat to financial and trust systems…on which the world economy depends."[13] For example, through online fraud, cyber crime groups based in Central and Eastern Europe have cost U.S. citizens and organizations an estimated $1 billion annually.[14] Attacks by these groups have increased in frequency and number in the last five years.[15] Cyber criminals operating in vulnerable states threaten U.S. cybersecurity through:

- *Asymmetric Cyber Attacks*: Criminal organizations operating within these states are capable of threatening critical infrastructure, defense networks, and large corporations in the United States and globally. Because the technology needed for cyber weapons is cheap and easily accessible, criminal groups and hacktivists are able to conduct sophisticated and dangerous cyber operations.[16] For example, between 2007 and 2011, a cyber crime gang based in Estonia hijacked approximately four million computers in over 100 countries and stole approximately $14 million. U.S. businesses and government agencies, including NASA, and over a half-million private citizens were among their targets.[17]

- *Connection to Drug Trafficking and Terrorism*: A July 2011 White House report stated that "virtually every transnational criminal organization and its enterprises are

connected and enabled by information systems technologies, making cyber crime a substantially more important concern."[18] Terrorist groups use these illegal markets to finance operations.[19] For example, Al-Qaeda and Hezbollah actively recruit and train computer specialists or hire preexisting groups to facilitate their cyber operations.[20]

Barriers to Effective Cyber Domain Defense

Vulnerable states are less able to independently implement necessary cybersecurity standards because of the high cost of cyber defense and declining defense budgets.

- *Cost of Cyber Defense*: The cost of developing secure cyber networks can quickly overwhelm the budgets of vulnerable states. For instance, the Department of Homeland Security requested $233.6 million in order to deploy one cyber program, EINSTEIN 3, and coordinate threat notification among federal networks.[21] Over the next four years, the United States will allocate $10.5 billion annually to information security programs.[22]

- *Declining Defense Budgets:* Defense budgets are expected to decline as a result of austerity measures throughout Europe, including those of Bulgaria, Romania, Slovenia, the Czech Republic, Belgium, and Latvia. For example:

  - Slovenia cut its defense budget by 20% from 2010 to 2011 and plans to cut another 7% in 2012.[23]

  - Romania's defense budget is projected to decrease 30% between 2012 and 2015.[24]

Weaknesses of Current U.S. Cybersecurity Policy

U.S. policy now focuses on denial, awareness, and technology transfers to like-minded states. Elements of these approaches are valuable components of a comprehensive cybersecurity policy, but are insufficient to address the threat of cyber crime in vulnerable states.

Denial: Deterring Cyber Attacks through Passive Defense

DARPA, USCYBERCOM, and Pentagon officials plan to accelerate the development of technology for the defense of U.S. military and government networks through R&D programs. DARPA expects a 73% increase in cyber research funding in 2012, from $120 million to $208 million.[25] The White House appropriated $6 billion to strengthen its networks against cyber attack in 2008.[26]

- *Strength*: A significant investment in domestic cyber defense technology will decrease the probability of a successful cyber attack. Current initiatives include developing more Information Sharing and Analysis Centers (ISACs), which collect and disseminate real-time data to government networks and businesses.[27] This

strategy will assist network analysts to detect and respond to cyber attacks before they can infiltrate secure networks or damage infrastructure.

- *Weakness*: The hardware and software necessary to instigate a cyber attack is inexpensive and easily accessible. Malicious code is much simpler to write than defense software—for instance, some defense software requires 10 million lines of code, versus approximately 125 lines for malware.[28] The cost of repeated network intrusion or infection attempts is low, and new malware can be developed much more quickly than additional network defenses. Therefore, exclusively investing in denial capability in U.S. networks will not hamper the operation of foreign cyber crime groups and their ability to penetrate the best network defenses. Former Deputy Secretary of Defense William Lynn warned that "a fortress mentality will not work" and will leave U.S. networks vulnerable to determined criminal or hacktivist groups.[29]

Awareness Campaigns

The U.S. government is currently investing in cybersecurity awareness plans, especially for government employees, individuals working with national critical infrastructure, and financial sector employees.[30] These plans include programs designed to educate individual users on the importance of installing updates, safeguarding passwords, and following security protocols.

- *Strength*: 85% of the threat to U.S. cybersecurity networks can be eliminated with proper cyber hygiene, personal strategies by which individual users can improve their computers' security.[31]

- *Weakness*: While awareness can reduce basic network vulnerabilities, corporations, government employees operating with .gov domains, and ordinary citizens will not receive timely notification of cyber threats. Organized, determined hackers will still be able to penetrate many networks' security software.

Guaranteed Technology Transfers to Like-Minded States

Recognizing the cyber threat from vulnerable states, the White House proposed unconditional capacity building for U.S. allies to improve network interoperability, response time, and resilience. This plan includes limited technology transfers, information exchange, and clarifying standard operating procedures between states.[32] Similarly, the Cybersecurity Act of 2012 (S. 2105) proposes prioritizing foreign aid to states planning to allocate that aid for cybersecurity development.[33]

- *Strength*: U.S. allies will be significantly better equipped to confront emerging cyber challenges. Response times to attacks will decrease as a result of regular cooperation between allies and interoperable network systems.

- *Weakness*: Offering unconditional technology transfers and network assistance does not encourage our allies to make cybersecurity a budgetary priority. Global austerity

measures threaten governments' defense budgets, and states that know they can rely on U.S. technology transfers will likely not invest as much in domestic R&D, cyber specialist training, or policy reform. A policy of guaranteed technology transfer will reduce global innovation and result in a larger budgetary burden for the United States. Similarly, the Cybersecurity Act of 2012 does not require states to make their own advancements in order to receive aid. Instead, they must simply express their intention to use the money for cyber capacity building.[34] Furthermore, hackers and organized criminal groups from any state can threaten U.S. networks. Therefore, cooperating with only the closest U.S. allies leaves networks open to a range of threats from other states.

Components of the above policies are necessary for a successful comprehensive cybersecurity strategy. However, they fail to account for declining defense budgets and the lack of independent cyber innovation programs among vulnerable states. An international framework that encourages states to rapidly upgrade their cybersecurity capability and law enforcement is a critical step in securing U.S. networks against cyber crime.

International Cyber Grade Framework

To encourage vulnerable states to make cybersecurity a priority, this brief proposes the creation of an international Cyber Grade Framework (CGF) paired with security incentives.

Targeted States

The primary purpose of this policy is to facilitate the implementation of rigorous cybersecurity standards in order to hinder the operation of cyber crime and hacktivist groups. It targets vulnerable states that desire to reduce cyber crime within their borders but are unwilling or unable to earmark sufficient government funds to do so. The CGF should apply primarily to vulnerable states, particularly those with a GDP of at least $10 billion. States that meet this budgetary guideline should have the capability to implement functional cybersecurity standards with the assistance of the international community.

- *Initial Region – Eastern Europe*: The initial stage of the policy will primarily target Eastern European NATO-member states. Eastern Europe is a known base for numerous cyber crime groups, which frequently target the U.S. financial sector.[35] In the past, the United States and NATO have successfully cooperated with Eastern European states primarily on short-term law enforcement operations to combat cyber crime. This collaboration establishes a promising precedent for more substantial long-term cooperation.

- *Future Policy Expansion – Central Asia, Africa and the Middle East*: Once the CGF has been tested with NATO members, it will be expanded to target regions outside of Eastern Europe, namely Central Asia, Africa, and the Middle East. Combating illegal cyber activity in these regions will significantly hinder the ability of money launderers, drug traffickers, and terrorists to operate.[36] NATO/U.S. relations with

these states are more sensitive than in Eastern Europe, but previous successful cooperation indicates the potential for a constructive relationship to combat transnational cyber crime.[37]

- *Exclusion of Russia and China:* Russia and China, which are suspected of cooperating with transnational groups to launch cyber attacks, would not be invited to participate in the proposed framework. This policy aims to assist vulnerable states that wish to cooperate closely with NATO and the United States and contribute to a more secure international cyber domain.

Baseline Assistance

States that do not participate in the CGF remain a threat to U.S. national security. To address this threat, NATO will:

- *Provide a Complementary Network Vulnerability Assessment:* A team of independent cyber analysts will complete a complementary assessment of the state's network vulnerability and the cost of intellectual property theft to the national economy.
- *Allow Limited Access to Cybersecurity Conferences:* NATO may also allow limited access to CGF cybersecurity conferences in order to encourage the state to opt into the voluntary international regulations.
- *Emphasize Compliance with Cybersecurity Norms:* Through diplomatic channels, the United States will emphasize that "cyber crime originating in or occurring within their jurisdiction is a serious crime with international implications," and they need to develop their legal systems to prosecute these crimes.[38]

Private Sector Framework

The CGF is based on a private-sector incentive model designed to encourage companies to implement cybersecurity standards without government mandates.[39] This model is the best approach to encourage higher cybersecurity standards in the absence of compulsory international cybersecurity standards. States will voluntarily adopt a grade's requirements in order to receive the associated incentives, encouraging them to make cybersecurity a priority. Simultaneously, this policy will strengthen participating states' ties with the international community, creating a more secure global network.

Grade One: The purpose of this grade is to foster cyber technology innovation to encourage rapid progress towards secure networks.

Requirements

- Increase cybersecurity R&D budget by 10% from the amount allocated in the year of accession to the CGF.
    - For a period of five years after achieving grade 1, the state must keep the cyber R&D budget at the required level, correcting for inflation.
    - Through increased R&D budget allocations, states will be capable of promoting independent domestic innovation. Additionally, they have the option of cooperating with existing research programs at the Cooperative Cyber Defence Center of Excellence (CCDCoE) in Estonia.[40]

Incentives

- Allow admittance to CGF international cybersecurity conferences.
- Implement cyber law enforcement training programs and provide international teams to assist in capacity building for law enforcement personnel.

Grade Two: The purpose of this grade is to facilitate intelligence sharing and install basic law enforcement/extradition standards to allow international cybersecurity cooperation.

Requirements

- Ensure compliance with CGF's security breach notification regulations.
    - CGF members are required to disclose information regarding criminal organizations that may threaten other member states in the CGF information clearinghouse, a new international body that will facilitate the exchange of information between states (see below).[41]
    - Members must implement a domestic framework within the government, to which corporations and individuals can report network breaches and cyber attacks.
- Implement minimum extradition guidelines.
    - Extradition standards are governed by Article 24 of the Budapest Convention on Cybercrime. States meet the standard by ratifying the treaty and adhering to its cybercriminal extradition guidelines.[42]
    - Officials appointed under the G-8 24/7 Cyber Crime Network will act as points of contact for intelligence exchange and extradition issues.[43] States that have not established a designated official will be required to do so.

Incentives

- Provide rapid reaction cyber teams following a cyber incident involving critical infrastructure to rebuild network defenses and improve resiliency.[44]

- Facilitate intelligence sharing between member states.

    - CGF will establish a clearinghouse for information on emerging cyber threats. Pertinent threat information will be transferred to states achieving Grade 2.

    - If information pertaining to a lower-grade state is received, the information may be shared at the discretion of the CGF clearinghouse and with the permission of the informing state.

- Supply limited technology transfers.

    - Technology transfers from the United States associated with this framework will be governed by the Department of Defense Technology Disclosure Policy.[45]

Grade Three: The purpose of this grade is to facilitate high-level cooperation between cyber law enforcement teams and military units to increase network resiliency and reduce incident response time.

Requirements

- Create a cybersecurity branch of law enforcement that is compliant with CGF standards. To achieve compliance, member states must have:

    - A national Computer Emergency Readiness Team, which can manage several domestic cyber threat databases and work with international teams in attribution operations;

    - A public notification system to inform non-government organizations of emerging cyber threats;

    - A database and notification system for authorized government employees to defend government networks and improve response time to cyber threats.[46]

- Engage in joint training of personnel with grade 3 states in order to increase the efficiency of inter-state operations and communication. Re-training for international network coordination personnel must occur every three years.

Incentives

- Participate in joint military operations with the United States and other grade 3 states. Exercises will focus on solidifying protocols for incident response and lessening the time necessary to restore network functionality following a variety of attacks.

- Expanded access to NATO rapid reaction cyber teams for a wider range of threats, including the cases of a denial of service cyber incident or information theft from government networks.

CGF Oversight and Compliance

NATO will administer the cybersecurity private-sector framework through a compliance organization modeled after the IAEA. This model was selected because of its applicability to a sensitive industry critical to national security. The organization will ensure compliance with enumerated standards.

- *Structure*: Within NATO, the CGF will be semi-autonomous, but it will report to NATO's North Atlantic Council. It will also act as a clearinghouse for cybersecurity information and coordinate with NATO's Cooperative Cyber Defence Centre of Excellence in Estonia for research and development.[47]

- *Main Administrative Bodies*: Two primary administrative bodies will design and execute policy for the organization:

    1) *General Conference*: The General Conference is composed of CGF member states. Once a state opts into the first cybersecurity grade, it receives one vote in the General Conference. This body will meet annually to approve measures recommended by the Board of Governors. Additionally, it will perform bi-annual audits of member states' security standards and report the findings to the Board of Governors for review. States may request that teams inspecting its facilities be accompanied by state representatives.

    2) *Board of Governors*: The Board of Governors will be composed of NATO Grade 3 states only. It will present policy and budget recommendations to the General Conference. It will be responsible for state suspensions and statute amendments and will meet five times per year to guide the General Conference.[48]

- *Member Accession Process*: States intending to join the oversight organization must meet the following requirements:

    1) Applicant state achieves one of the three cybersecurity grades as defined by the aforementioned regulations and verified by the General Conference.

    2) NATO's North Atlantic Council approves the application with a 2/3 majority.

    3) General Conference approves the application with a 2/3 majority.

- *Cost of Membership*: States will be required to pay low dues for membership in the CGF in order to cover approximately one-half of the organization's costs. NATO will pay the remaining costs, which will be significantly less expensive than the cost of the free technology transfers, rapid reaction teams, and legal training currently in place.

Strengths of the Proposed Cybersecurity Framework Policy

The CGF uses incentives to foster greater cybersecurity capability and provides the following benefits:

- *Cost Effectiveness*: Rather than providing free technology transfer to numerous states in order to update their cybersecurity systems, this policy requires states to make cybersecurity a domestic budget priority. Many of the costs of research and installation will be borne by participating states, while NATO will provide the expertise necessary to ensure the most effective practices and infrastructure are used.

- *Promotes International Innovation*: States will invest in their own R&D projects, prompting global innovation. The United States and other key cyber powers will not be alone in developing new technologies and methods, allowing for a more versatile, resilient global cybersecurity network.

- *Solidifies International Cybersecurity Norms*: Currently international cybersecurity norms regarding cyber criminals and hacktivists are absent or vague. Implementing this framework will clarify and bolster these norms, allowing NATO to hold states to an international standard and encourage more international cooperation on issues pertaining to cyber crime.

- *Increases Network Communication Speed*: In order to reach the highest cybersecurity grade, states must participate in joint training to facilitate intelligence sharing, early warning systems, and joint cyber operations. Joint personnel training will decrease response time and increase resilience of all member states' networks.

Possible Objections to the Proposal

- *Objection*: States will not to opt into the CGF because they fear U.S. interference in their networks.

  Response: The two-stage policy is designed to reassure non-NATO members that the CGF can be implemented without U.S. interference in sensitive network technology. Additionally, Eastern European states have successfully cooperated with the United States and NATO, yielding positive results.

  - *Estonia:* Following the 2007 Denial of Service attacks, which disrupted the Estonian financial sector networks, Estonia invited the United States to assist with damage control and rehabilitation of the networks. Since 2007, Estonia and the United States have worked with NATO to establish the Cooperative Cyber Defense Centre of Excellence (CCD COE) to promote cyber technology R&D.

  - *Slovenia:* From 2007 to 2011, the FBI worked with the Slovenian Cyber Emergency Readiness Team (SI-CERT) to take down an international botnet, which threatened the networks of several countries. The criminals operating the botnet were identified and convicted because of cooperation between the two agencies.[49]

- *Objection*: The United States will not allow CGF teams to inspect its cybersecurity structures to ensure compliance with CGF regulations.

  Response: International compliance teams have been used previously in highly sensitive military sectors, such as nuclear weaponry. For example, in 1967 the United States agreed to "permit the International Atomic Energy Agency to apply its safeguards to all nuclear activities in the United States–excluding only those with direct national security significance."[50] Inspection teams will always be accompanied by representatives of the member state if requested.[51] Furthermore, the CGF inspection teams will not need access to sensitive cyber technology. Rather, teams will perform detailed inspections of law enforcement agencies, general budgets, and extradition records.

- *Objection:* The United States and NATO will be reluctant to provide technology transfers to states developing cyber capabilities.

  Response: Current U.S. and NATO policies provide technology transfers to states developing their cybersecurity capabilities. This proposal differs from precedent only in that the United States and NATO will not be providing technology transfers freely but rather as an incentive to reward compliance with the voluntary regulations. Currently, NATO-verified Centers of Excellence develop and transfer technology to member states. Additionally, the DoD Defense Technology Security Administration approves approximately 30,000 export licenses annually for controlled hardware and technology.[52]

Conclusion

Cybersecurity is vital to preserving stability in the financial sector, military readiness, and critical infrastructure. States must rapidly advance their cybersecurity capabilities to keep pace with growing challenges. Most states are currently at dramatically different levels of cyber capability, impeding their ability to communicate and participate in joint operations.

The CGF will encourage states to prioritize cybersecurity in their budgets and meet voluntary regulations to receive security incentives. This proposal will foster innovation and facilitate the transition to a higher level of cybersecurity, cooperation, and law enforcement capability. The advancements from the CGF will create more secure global networks, capable of confronting a critical 21st century threat.

---

[1] "Symantec Report Finds Cyber Threats Skyrocket in Volume and Sophistication," *Symantec Corporation*, April 5, 2011, http://www.symantec.com/about/news/release/article.jsp?prid=20110404_03.; Michael Cooney, "US cyber chief says cloud computing can manage serious cyber threats," *Network World*, November 7, 2011, http://www.networkworld.com/news/2011/110711-cyberchief-cyberthreats-252844.html?hpg1=bn.

[2] A botnet is a "computer robot," which is created when a user intentionally or unintentionally downloads malware to his computer. A "botherder" or "botmaster" is then able to control that computer from his base computer. Botnets

can contain hundreds of thousands of computers, which are then capable of instigating denial-of-service attacks, for example. "Bots and Botnets—A Growing Threat," *Norton Antivirus*, accessed January 20, 2012, http://us.norton.com/theme.jsp?themeid=botnet; Dean Wilson, "US Shuts Down a Major Cyber Crime Botnet," *The Inquirer*, April 14, 2011, http://www.theinquirer.net/inquirer/news/2043439/shuts-major-cyber-theft-botnet.

[3] *Cybersecurity: Responding to the Threat of Cyber Crime on Terrorism, Testimony before the Senate Judiciary Committee Subcommittee on Crime and Terrorism*, 112th Congress (April 2011) (Statement of Gordon M. Snow, Assistant Director, Cyber Division, FBI), http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism.

[4] Elizabeth Montalbano, "Federal Cyber Attacks Rose 39% In 2010," *InformationWeek*, March 23, 2011, http://www.informationweek.com/news/government/security/229400156.

[5] Lolita C. Baldor, "Pentagon spends $100 million on cyber attacks," *MSNBC Security*, April 7, 2009, http://www.msnbc.msn.com/id/30090749/ns/technology_and_science-security/t/pentagon-spends-million-cyber-attacks/#.T1ZL5_XksW1.

[6] "CSIS Cybersecurity Policy Debate Series: U.S. Cybersecurity Policy and the Role of U.S. CYBERCOM," *Center for Strategic and International Studies*, June 3, 2010, http://csis.org/files/attachments/100603csis-alexander.pdf, 5.

[7] Stewart Baker et al., "In the Crossfire: Critical Infrastructure in the Age of Cyber War," *McAfee, Inc.*, 2009, http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf, 10.

[8] U.S. Department of Defense, John D. Banusiewicz, "Lynn Outlines New Cybersecurity Effort," June 16, 2011, http://www.defense.gov/news/newsarticle.aspx?id=64349.

[9] Matthew Hansen, "U.S. on Offense in Cyberwar?" *Omaha World-Herald*, November 20, 2011, www.omaha.com/article/20111120/NEWS01/711209927.

[10] Shawn Henry, "Responding to the Cyber Threat" (speech presented at the Information Systems Security Association International Conference, Baltimore, Maryland, October 20, 2011).

[11] Operation Shady RAT (Remote Access Tool) was an ongoing cyber attack initiated in 2006 and reported in 2011 by McAfee. The Republic of China is widely accepted as the likely perpetrator. A large number of the victim companies and organizations did not realize their networks had been compromised. Dmitri Alperovitch, "Revealed: Operation Shady RAT," *McAfee Inc.*, March 6, 2012, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

[12] Gordon M. Snow, *Cybersecurity: Responding to the Threat of Cyber Crime on Terrorism*.

[13] Kathleen Hickey, "How International Cyber Crime Threatens National Security," *Government Computer News*, July 27, 2011, http://gcn.com/articles/2011/07/27/international-cyber-crime-threat-to-us.aspx.

[14] U.S. White House, "Strategy to Combat Transnational Organized Crime," Accessed March 6, 2012, http://www.whitehouse.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf, 7.

[15] Gerry Smith, "Cyber-Crimes Pose 'Existential' Threat, FBI Warns," *Huffington Post*, January 12, 2012, http://www.huffingtonpost.com/2012/01/12/cyber-threats_n_1202026.html.

[16] U.S. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011, http://www.defense.gov/news/d20110714cyber.pdf, 3.

[17] "US Shuts Down Cyber Crime Gang," *Irish Times*, November 10, 2011, http://www.irishtimes.com/newspaper/breaking/2011/1110/breaking53.html.

[18] U.S. White House, "Strategy to Combat Transnational Organized Crime."

[19] Clay Wilson, *Botnets, Cyber Crime, and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*, CRS Report for Congress (The Library of Congress: Congressional Research Service, January 29, 2008), http://www.fas.org/sgp/crs/terror/RL32114.pdf, 2, 30.

[20] Raphael F. Perl, *Terrorist Use of the Internet: Threat, Issues, and Options for International Co-operation* (Organization for Security and Cooperation in Europe, April 7, 2008), http://www.osce.org/atu/31428.; "Cyber Security and Terrorism," *Interfor*, March 6, 2012, http://www.interforinc.com/FileLib%5CCyberterrorism.pdf, 3.

[21] U.S. Department of Homeland Security, "FY 2012 Budget in Brief," Retrieved January 12, 2012, http://www.dhs.gov/xlibrary/assets/budget-bib-fy2012.pdf, 11.

[22] "Cyber Security and Terrorism."

[23] "Defence Budget (Slovenia) - Sentinel Security Assessment - The Balkans," *Jane's Information Group*, December 26, 2011, http://articles.janes.com/extracts/extract/balksu/slovs090.html.

[24] "Research and Markets: The Romanian Defense Industry – Market Opportunities and Entry Strategies Analyses and Forecasts to 2015," *Business Wire*, December 27, 2011,

http://www.businesswire.com/news/home/20110506005294/en/Research-Markets-Romanian-Defense-Industry---Market.
[25] Jim Wolf, "U.S. Says Will Boost Its Cyber Arsenal," *Reuters,* November 7, 2011, http://www.reuters.com/article/2011/11/07/us-cyber-usa-offensive-idUSTRE7A640520111107.
[26] Bobbie Johnson, "NATO says cyber warfare poses as great a threat as a missile attack," *The Guardian,* March 5, 2008, http://www.guardian.co.uk/technology/2008/mar/06/hitechcrime.uksecurity.
[27] U.S. Department of Homeland Security, "Blueprint for a Secure Cyber Future," November 2011, http://www.cyber.st.dhs.gov/wp-content/uploads/2011/12/blueprint-for-a-secure-cyber-future.pdf, 7.
[28] Jim Wolf, "U.S. Says Will Boost Its Cyber Arsenal," *Reuters,* November 7, 2011, http://www.reuters.com/article/2011/11/07/us-cyber-usa-offensive-idUSTRE7A640520111107.
[29] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010).
[30] U.S. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace."
[31] U.S. House of Representatives, "Recommendations of the House Republican Cybersecurity Task Force," October 2011, http://thornberry.house.gov/UploadedFiles/CSTF_Final_Recommendations.pdf, 12.
[32] U.S. White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, 19.
[33] Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012) http://www.hsgac.senate.gov/imo/media/doc/CYBER%20The%20Cybersecurity%20Act%20of%202012%20final.pdf.
[34] Ibid.
[35] Clay Wilson, *Botnets, Cyber Crime, and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*.
[36] Ibid.
[37] For example, the 2004 Istanbul Cooperation Initiative (ICI) established bilateral military cooperation between NATO and states in the Middle East. Members include Bahrain, Qatar, Kuwait, and the UAE. The initiative promotes military interoperability, intelligence sharing, and participation in NATO exercises. Additionally, in February 2012, the U.S. Air Force and Kyrgyzstani Ministry of Defense exchanged intelligence on sensitive systems and tactics, including chemical weapons and CBRNE procedures. This cooperation continued a precedent of intelligence sharing between the United States and Kyrgyzstan. Istanbul Cooperation Initiative (ICI), November 18, 2011, http://www.nato.int/cps/en/SID-52237F1C-F7242949/natolive/topics_58787.htm?; Lynsie Nichols, "US, Kyrgyz share EOD, CBRNE Techniques," February 27, 2012, http://www.manas.afcent.af.mil/news/story.asp?id=123291439.
[38] U.S. House of Representatives, "Recommendations of the House Republican Cybersecurity Task Force," October 2011, http://thornberry.house.gov/UploadedFiles/CSTF_Final_Recommendations.pdf, 18.
[39] U.S. House of Representatives, "Recommendations of the House Republican Cybersecurity Task Force."
[40] CCDCoE was founded in 2008 and promotes the development of cyber technology. Based in Tallinn, Estonia, it is sponsored by several states including Estonia, the United States, Latvia, Lithuania, Germany, Italy, and Poland. NATO, and Active Command Transformation specifically, uses this facility to develop new cyber technology and policy. NATO Cooperative Cyber Defense Center of Excellence, http://www.ccdcoe.org/.
[41] See "CGF Oversight and Compliance" section for additional information.
[42] Convention on Cybercrime, November 23, 2001, UNTC I-40916.
[43] Raphael F. Perl, "Terrorist Use of the Internet: Threat, Issues, and Options for International Co-operation."
[44] National Critical Infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Critical Infrastructures Protection Act of 2001, §5195 (2001).
[45] The National Disclosure Policy provides guidelines for the disclosure of classified military information (CMI) to foreign governments and/or organizations. U.S. Department of Defense, "National Disclosure Policy: Chapter 3 – Technology Transfer and Disclosure," October 3, 2003, http://www.dsca.mil/samm/Chapter%2003%20-%20Technology%20Transfer%20and%20Disclosure.pdf.
[46] See the U.S. Federal Vulnerability Knowledgebase. U.S. Computer Emergency Readiness Team, "Analytical Tools and Programs: Government Users," February 24, 2012, http://www.us-cert.gov/federal/analytical.html.
[47] "NATO and Cyberdefence," September 16, 2011, http://www.nato.int/cps/en/SID-63B85F2D-2CA198C8/natolive/topics_78170.htm?.

[48] Suspensions can occur when a state initially implements the guidelines necessary for a grade, but it fails to maintain the provision requirements. They may also occur if a state grossly endangers the security of CGF members' networks via cooperation with transnational crime groups or otherwise. The board of governors has the option of demoting the state's grade or suspending it from the CGF.
[49] Slovenian Computer Emergency Readiness Team (SI-CERT), "SI-CERT Prejel Priznanje FBI," January 17, 2012, http://www.cert.si/.
[50] Agreement between the United States of America and the International Atomic Energy Agency for the Application of Safeguards in the United States (and Protocol Thereto), November 18, 1977, TIAS 6839, http://www.state.gov/t/isn/5209.htm.
[51] Ibid.
[52] U.S. Department of Defense, "Defense Technology Security Administration," http://www.dtsa.mil/.