International Cyberspace Strategies

Kathryn Stephens, NSCI;
Larry K. McKee, Jr., NSCI
June 28, 2010

National Security Cyberspace Institute, Inc. (NSCI)

Through the combination of research and education, NSCI supports public and private clients aiming to increase cyberspace awareness, interest, knowledge, and/or capabilities. NSCI is committed to helping increase security in cyberspace whenever and wherever possible. NSCI publishes a bi-weekly newsletter (*CyberPro*), has published numerous whitepapers on various cyberspace topics, maintains an online cyber reference library, and has established an email distribution list for sharing cyber-related resumes to interested parties. NSCI is a small, veteran-owned business headquartered in Virginia.

Introduction

According to Dave DeWalt, chief executive and president of the network security firm McAfee, 20 countries are now engaged in a cyber arms race. DeWalt goes on to say at least five countries – the United States, China, Russia, Israel and France – now have offensive cyber capabilities and have moved from a “defensive posture to a more offensive posture." McAfee recently conducted a survey which found that there has been more than a 500 percent increase in net new malware over the past year, and that 60 percent of IT security executives surveyed believed that representatives of foreign governments were involved in infrastructure infiltrations. The survey also found that attacks are now costing $6.3 million a day around the world. “Despite the potential damage, governments appeared to be lagging behind in taking measures to get private sector to protect their web infrastructure."[1]

Perhaps because of these trends, there appears to be a recent uptick in interest in international collaboration and information sharing. For example, 1500 cybersecurity experts from 23 countries met in Lille, France, last year for the International Forum on Cyber Crime. Participants discussed identity theft, data piracy, virus attacks, electronic fraud, network penetration, botnets, and espionage, and hoped to foster international collaboration. Attendees also discussed the difficulties from American companies such as YouTube and Facebook expanding into Europe. The Internet is treated very differently in Europe than in the U.S., and the EU does not currently have a comprehensive cybersecurity strategy or standardized personal privacy laws from member nations.[2] Other conferences and symposiums convened to discuss cyber security include the first Worldwide Cybersecurity Summit hosted by the EastWest Institute in Dallas, Texas, and the International Conference on Cyber Security (ICCS) series of annual meetings.

Further evidence of increasing international interest in the cyber domain is the standup of centralized agencies dedicated to cyber security. These include Singapore, South Korea, Australia, Malaysia, Japan, and Hong Kong.[3]

With this increasing international interest, we thought it timely to provide a "current intel" update on a number of countries' approaches, strategies, and organizations dedicated to improving cyber security. This is a follow-on to our May 17th "International Cyber Considerations" paper, which discussed the top 10 internet-using countries, primarily focusing on economic, industrial, technological, and military capabilities that might make them lucrative targets of cyber attack. The countries we've chosen for this latest update are Australia, France, Canada, the United Kingdom, the United States, Russia, and China. We also provide short discussions of recent developments within the UN and NATO.

[1] Neo, H. M. (2010, January 28). *China, US, Russia in cyber arms race: net security chief.* Retrieved June 10, 2010, from Google News: http://www.google.com/hostednews/afp/article/ALeqM5gBI-UmsuwvR6i-mxl5TDGvDuGtrw

[2] Mann, J. (2010, March 31). *Europe Declares War on Cyber Crime.* Retrieved June 10, 2010, from The New New Internet: http://www.thenewnewinternet.com/2010/03/31/europe-declares-war-on-cyber-crime/

[3] *Cyber security of national importance.* (2010, May 26). Retrieved June 10, 2010, from Bangkok Post: http://www.bangkokpost.com/tech/technews/37745/cyber-security-of-national-importance

Australia

The Australian Government launched its Cyber Security Strategy on November 23, 2009. The Australian Attorney General is in charge of cyber security policy for the government, with a Cyber Security Policy and Coordination (CSPC) Committee leading interdepartmental coordination across the Government. The Australian Government defines cyber security as "measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means" and the overall aim of Australia's cyber security policy is "the maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximizes the benefits of the digital economy."[4] Australia's cyber security policy aims to confront and manage cyber threats and is based on guiding principles which include:

- national leadership; shared responsibilities;
- partnerships between the Australian government and private sector;
- international engagement;
- risk management; and
- policies that protect the individual's right to privacy

The Australian Government is focusing on the following cyber security priorities:

- improving the detection and response to cyber threats;
- educating Australians to better protect themselves;
- partnering with businesses;
- modeling best practices in protecting government systems;
- promoting a secure and trusted global electronic operating environment;
- maintaining a legal framework and capabilities to prosecute cyber crime; and
- promoting the development of skilled cyber security workers.

Two organizations are central to Australia's cyber security strategy. CERT Australia, which began operations in early 2010, is the source of cyber information for Australia, and provides access to threat information to Australian citizens. CERT Australia l also coordinates response during a cyber security incident. The Cyber Security Operations Center (CSOC) provides threat detection and mitigation for the Australian Government, as well as situational awareness.[5] Australia has also established an annual national Cyber Security Awareness Week.

Australia has been in the news recently, promoting a voluntary code of conduct for ISPs in the country. The Australian Internet Industry Association is asking ISPs to adopt the code that would require them to better educate customers, offer better online protection, and quarantine infected users. Security firm Imperva says that temporarily blocking an infected user would give customers more confidence online, and would also reduce the levels of zombie infections. Imperva is urging other nations to adopt a similar code of conduct.[6] Internet Industry Association CEO Peter Coroneos says that the new policy is like requiring drivers to replace their tires or brakes

[4] *Cyber Security.* (2009, November 16). Retrieved June 10, 2010, from Australian Government Attorney-General's Department: http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurityy
[5] *Cyber Security.* (2009, November 16). Retrieved June 10, 2010, from Australian Government Attorney-General's Department: http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurityy
[6] Ashford, W. (2010, June 9). *Australian ISP code could defeat new generation of DDoS attacks, says Imperva.* Retrieved June 10, 2010, from ComputerWeekly.com: http://www.computerweekly.com/Articles/2010/06/09/241511/Australian-ISP-code-could-defeat-new-generation-of-DDoS-attacks-says.htm

when they have gone bad, and says that “Internet users have a responsibility not only to themselves, but also to other users on the Internet."[7]

According to an article from The New New Internet, the Australian Communications and Media Authority currently maintains a list of blacklisted sites, and requires Australian ISPs to filter these sites. A leaked copy of the list in 2008 contained 2,395 sites, but the Australian government says that it will expand the list to 10,000 sites or more. Australia’s Communications Minister Stephen Conroy says that the blacklist targets only illegal sites, but some feel that the scope of the censored content is too broad.[8]

Much like the U.S. Department of Defense and Department of Homeland Security, the Australian Government is looking to quickly recruit cybersecurity experts for government positions. Last January, Defense Minister John Faulkner announced that the Ministry of Defense would recruit 130 cybersecurity experts to work at Australia’s Cyber Security Operations Center. The recruits would include IT engineers, programmers and analysts. Faulkner said that “cyberspace is a battlefield” and that “cybersecurity is one of the government’s top national security priorities."[9]

France

In 2008, a French *White Paper on Defence and National Security* identified cyber threats as a significant threat to France. In response to the recommendations found in the paper, the French government announced the creation of the French Network and Information Security Agency (FNISA) on July 7, 2009. The new agency is responsible for the following areas:

- detection and response to attacks;
- continuous surveillance of sensitive government networks;
- prevention of threats through supporting the development of trusted products and services;
- reliable advice and support to the French government; and
- keeping companies and the general public informed about cyber threats and means of protection.[10]

The French Centre of Expertise for Government Response and Treatment of Computer Attacks (CERTA) is responsible for helping the government implement defenses and resolve cyber incidents and attacks. CERTA focuses on vulnerability detection for the French government, and assisting in developing better defenses to protect government systems from future incidents.[11]

France is one of several nations that recently called for users to stop using Internet Explorer. Although Microsoft recommended that users upgrade to Internet Explorer 8, France’s CERTA asked that all Internet users refrain from using any recent version of Internet Explorer.[12] Patrick Pailloux, director general of France’s Network and Information Security Agency (FNISA), recently attended the first Worldwide Cybersecurity Summit hosted by the EastWest Institute in Dallas, Texas. Pailloux said that France wants to see an increase in exchanging information

[7] Mann, J. (2010, June 7). *Australians Look to Block Off Zombie Computers.* Retrieved June 10, 2010, from The New New Internet: http://www.thenewnewinternet.com/2010/06/07/australians-look-to-block-off-zombie-computers/

[8] Tuutti, C. (2010, March 30). *U.S. Criticizes Australia's Attempts to Censor Cyberspace.* Retrieved June 10, 2010, from The New New Internet: http://www.thenewnewinternet.com/2010/03/30/u-s-criticizes-australias-attempts-to-censor-cyberspace/

[9] UPI (2010, January 21). Australia recruits cybersecurity experts. Retrieved June 10, 2010 from http://www.upi.com/Business_News/Security-Industry/2010/01/21/Australia-recruits-cybersecurity-experts/UPI-66471264091354/ .

[10] *The French Network and Information Security Agency.* (2009). Retrieved June 10, 2010, from ANSSI: www.ssi.gouv.fr/site_article76.html

[11] *CERTA.* (2010). Retrieved June 10, 2010, from ANSSI: www.ssi.gouv.fr/site_rubrique48.html

[12] *French Government calls on Internet users to abandon Internet Explorer.* (2010, January 19). Retrieved June 10, 2010, from New.com.au: http://www.news.com.au/technology/french-government-calls-on-internet-users-to-abandon-internet-explorer/story-e6frfro0-1225821078692

internationally about threats, vulnerabilities and attacks. Pailloux also said that the nations could work together to conduct joint cyber defense exercises.[13]

France has also made news lately because of its controversial policies on Internet censorship. French President Sarkozy's administration created an agency called the Higher Authority for the Distribution of Works and the Protection of Copyright on the Internet which requires ISPs to monitor French users for copyrighted music and video. ISPs must send warnings to users, and if ignored, users could be taken to court and have their internet service cut off. The original legislation of the bill did not even include a court hearing for offenders, but free speech activists pushed for due legal process in the legislation. Experts are concerned about how much the ISPs are required to monitor, and if those monitoring privileges could be abused.[14]

Canada

Several reports claim that Canada may have the least developed cyber security strategy. Dragos Ruiu, the organizer of the CanSecWest security conference in Vancouver, says that Canada "is woefully unprepared for a cyber attack on its infrastructure." [15] While governments worldwide have made cyber security a priority, and have altered their defense spending and organization, "Canada has no formal plans about how to respond to a coordinated attack by hackers."[16]

Christine Csversko, a spokeswoman for Public Safety Minister Vic Toews, said that the Canadian government is aware of the danger from Internet threats, and also confirmed that Canada is working on a national cyber security strategy that would promote education about cyber threats, and provide protection for government systems. Csversko said that several Canadian departments including the Royal Canadian Mounted Police, the Communications Security Establishment and the Canadian Security Intelligence Service are all responsible for responding during a cyber incident. Rafal Rohozinski, chief executive of Ottawa's SecDev Group[17], says that the Canadian government is having a hard time developing a cyber plan because the private sector owns so much of cyberspace that getting "all of the pieces together is challenging." Rohozinski also said that instead of every nation developing a cyber response plan, it would be better for nations to work together to define how cyber attacks can be used and what type of response is acceptable from a nation that has been hacked.[18]

The Canadian Advanced Technology Alliance (CATA Alliance) thinks that Canada should appoint a federal cyber security coordinator, like President Obama has done in the United States, in order to make better use of the security expertise in Canada. Kevin Wennekes, CATA Alliance's vice-president of research, says that Canada "lacks a centralized effort to raise awareness and create and advance what is a solid base of security knowledge in the IT industry." Wennekes explains that the Canadian government has a large community of IT specialists, but that information is not shared between departments. CATA Alliance launched two new initiatives last November. The

[13] *Cybersecurity meet ends with calls for global cooperation* . (2010, May 5). Retrieved June 10, 2010, from Space War: http://www.spacewar.com/reports/Cybersecurity_meet_ends_with_calls_for_global_cooperation_999.html

[14] MacKinnon, R. (2010, January 13). *Will Google stand up to France and Italy, too?* Retrieved June 10, 2010, from Guardian.co.uk: http://www.guardian.co.uk/commentisfree/libertycentral/2010/jan/13/google-china-western-internet-freedom

[15] Bradbury, D. (2010, April 28). *Where is Canada's cyber security strategy?* Retrieved June 10, 2010, from Geek Town: www.geektown.ca/2010/04/where-is-canadas-cyber-security-strategy.html

[16] Piliece, V. (2010, March 23). *Canada unprepared for massive cyber-attack: Expert.* Retrieved June 10, 2010, from Montreal Gazette: http://www.montrealgazette.com/technology/Canada+unprepared+massive+cyber+attack+Expert/2717868/story.html

[17] The SecDev Group is a Canadian company with a global mission to engage with complex problems of insecurity and violence. SecDev.cyber focuses on the emerging domain of cyberspace providing state-of-the-art analytical and investigation capabilities. The SecDev Group is headquartered in Ottawa, Canada, with a global network of over 45 partner institutions.

[18] Piliece, V. (2010, March 23). *Canada unprepared for massive cyber-attack: Expert.* Retrieved June 10, 2010, from Montreal Gazette: http://www.montrealgazette.com/technology/Canada+unprepared+massive+cyber+attack+Expert/2717868/story.html

first is a ten year technology roadmap for first responders who must handle sensitive data, and the other is a review of the Canadian security space by updating a database of advanced security companies.[19]

Last month, Canada amended the *Personal Information Protection Act* (PIPA) and added the requirement that organizations notify the Information and Privacy Commissioner of incidents that involve the loss of personal information that could cause harm to an individual. The amendments also give the Commissioner power to require organizations to notify the individuals at risk.[20]

United Kingdom

In June 2009, the UK Office of Cyber Security and the UK Cyber Security Operations Centre published the Cyber Security Strategy of the United Kingdom, which outlines the UK government's approach to cyber security in order to work towards the UK vision: "to understand and address the risks, to reduce the benefits to criminals and terrorists, and to seize opportunities in cyber space to enhance the UK's overall security and resilience." In the publication, the UK government committed to establishing a cross-government program that would be responsible for funding the development of innovative technologies and also working closer with the public sector and international partners. The UK government set up an Office of Cyber Security (OCS) to provide cybersecurity leadership, and also created a Cyber Security Operations Centre (CSOC) to coordinate incident response, promote user education, and provide advice to businesses about Internet risks and threats.[21]

The UK government hopes to take advantage of cyberspace to gather intelligence on threats, promote support for UK policies, and to intervene against adversaries. The Cyber Security Strategy of the United Kingdom also attempts to put a plan in place to develop doctrine and policy, develop governance and decision making, and to enhance technical and human capabilities.[22]

The UK has also conducted extensive research on how much cyber crime is affecting the UK, and what preventive measures Internet users could take to better protect themselves and their information. The UK Serious Organised Crime Agency estimates that online fraud is costing UK Internet users around £3.5 billion a year, and research by VeriSign says that 11 percent of the UK's Internet users were victims of fraud in the past year.[23]

The UK, like the United States, is looking to recruit and hire future cyber warriors for government positions. The United Kingdom has started to use public competitions to find talented recruits. The Cyber Security Challenge, which is backed by UK commercial, academic and public sector organizations, tests the cyber security skills of participants in order to identify future cyber security professionals. The competition includes games in eight key skill areas such as digital forensics, network analysis and logical thinking. Those who perform well in the games are invited to participate in a second challenge including a technical assault course and face-to-face tests. Top performers in the competition will be awarded prizes including scholarships, training courses and mentoring in hopes that the top performers will land government jobs where their skills could be used.[24] A survey from the SANS Institute said that 90 percent of the respondents from the security industry said that they found it difficult to

[19] Lau, K. (2010, January 26). *Canada needs cyber security czar: CATA Alliance.* Retrieved June 10, 2010, from Network World: http://www.networkworld.com/news/2010/012610-canada-needs-cyber-security-czar.html

[20] Office of the Privacy Commissioner of Alberta. (2010, May 3). *New breach notification requirements in effect in Canada.* Retrieved June 10, 2010, from DataBreaches.net: www.databreaches.net/?p=11516

[21] UK Office of Cyber Security. (2009, June). *CabinetOffice.gov.uk.* Retrieved June 10, 2010, from Cyber Security Strategy of the United Kingdom: www.cabinetoffice.gov.uk/media/216620/css0906.pdf

[22] UK Office of Cyber Security. (2009, June). *CabinetOffice.gov.uk.* Retrieved June 10, 2010, from Cyber Security Strategy of the United Kingdom: www.cabinetoffice.gov.uk/media/216620/css0906.pdf

[23] Ashford, W. (2010, June 1). *UK internet users need to be more vigilant as online fraud hits £3.5bn, says VeriSign.* Retrieved June 10, 2010, from Computer Weekly: http://www.computerweekly.com/Articles/2010/06/01/241410/UK-internet-users-need-to-be-more-vigilant-as-online-fraud-hits-1633.5bn-says.htm

[24] *UK launches competition to find cyber security experts.* (2010, April 27). Retrieved June 10, 2010, from BBC News: http://news.bbc.co.uk/2/hi/technology/8645041.stm

recruit cyber security workers, and the respondents identified the fields of strategy, policy guidance, risk management, incident response and threat management as the most difficult to staff.[25]

Earlier this year, the UK government announced that it would revamp its strategy for fighting cybercrime. Junior Home Office minister Alan Campbell said the new strategy would help build confidence in online government services, and would also help target financial criminals by putting the new Office for Cyber Security at the forefront of fighting cybercrime. The new strategy has five key elements including better coordination across government departments, and providing a better law enforcement response to electronic crime. Other goals of the new strategy include raising public confidence and building closer ties with industry. The UK government has also committed to working with other nations to stop cybercrime.[26]

UK domain registry Nominet made news earlier this year by announcing that they would implement DNS Security Extensions (DNSSEC), a security protocol that uses public key cryptography to digitally sign DNS records in order to stop attacks such as cache poisoning. Nominet will start by signing the .uk top-level domain, and will eventually move to the .co.uk and .org.uk domains later this year.[27] The UK Technology Strategy Board is also working to develop a cyber test range that will research and test cybersecurity threats on large-scale networks. The range will allow the UK to conduct cyber experiments and assess infrastructure assurance as well as new concepts that could help combat cyber threats.

United States

The United States' cyber security strategy is based largely on two documents: the Comprehensive National Cybersecurity Initiative (CNCI) and the Cyberspace Policy Review. Both documents include important initiatives and recommendations for the U.S. government as it is creating a national cyber security strategy. There are three major goals from the CNCI which include: to establish a front line of defense against today's immediate threats; to defend against the full spectrum of threats; and to strengthen the future cybersecurity environment. Each of these goals is supported by a number of key initiatives. The CNCI calls on the government to manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections, which includes consolidating the Federal Government's external access points. The government must also deploy an intrusion detection system of sensors across the Federal enterprise which will help to identify when unauthorized users have accessed government networks. The CNCI further recommends that the government pursue deployment of intrusion prevention systems across the Federal enterprise, which is part of the Einstein 4 program from DHS, and will allow the government to identify and stop malicious network traffic entering or leaving government networks.

The CNCI also calls for better coordination of research and development efforts funded by the U.S. government. The U.S. also needs to connect current cyber ops centers and enable better information sharing in order to enhance situational awareness. The report calls for the development of a government-wide cyber counterintelligence plan, and for increased security on classified networks. The report also discusses the need for expanded cyber education and an adequately established Federal cybersecurity career field. The CNCI says that the U.S. government must define and develop new technologies, strategies and programs as well as enduring deterrence strategies. The U.S. also needs a multi-pronged approach to global supply chain risk management, and a better definition of the Federal role in critical infrastructure defense.[28]

[25] Ashford, W. (2010, April 27). *UK Cyber Security Challenge to find next generation of security experts.* Retrieved June 10, 2010, from Computer Weekly: http://www.computerweekly.com/Articles/2010/04/27/241057/UK-Cyber-Security-Challenge-to-find-next-generation-of-security.htm

[26] Leyden, J. (2010, March 3). *UK.gov revamps cybercrime strategy.* Retrieved June 10, 2010, from The Register: http://www.theregister.co.uk/2010/03/31/uk_cybercrime_strategy/

[27] Kirk, J. (2010, March 2). *UK registry to tighten web security.* Retrieved June 10, 2010, from Tech World: http://news.techworld.com/security/3213803/uk-registry-to-tighten-web-security

[28] *The Comprehensive National Cybersecurity Initiative*. (n.d.). Retrieved June 16, 2010, from WhiteHouse.gov: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

The Cyberspace Policy Review, a 60-day review of federal cybersecurity efforts ordered by President Obama, also has several recommendations for the government. The report calls on the government to appoint a cybersecurity policy official responsible for coordinating national cybersecurity policies, and also designate cybersecurity as one of the president's key priorities including performance metrics. The report also calls for better cooperation among federal agencies including information sharing and collaboration on cyber security. The report calls for a public awareness and education campaign that will promote cybersecurity. The report also discussed the need for an international cybersecurity policy framework that will help to improve international partnerships and deter cyber attacks. The government was also asked to prepare a cybersecurity incident response plan, and address privacy and civil liberty issues.[29]

Earlier this year, a report from McAfee and the Center for Strategic and International Studies found that fewer executives in U.S. critical infrastructure industries thought they were subject to cybersecurity regulations compared to their global counterparts. Seventy two percent of executives in the United States said they were subject to regulations, compared with 92 percent in China and Germany, 97 percent in India, and 86 percent overall.[30]

Gen. Keith Alexander, the new head of the U.S. Cyber Command, says that the U.S. military has "virtually no situational awareness that would enable it to know when a cyber attack is underway" in an address at the Center for Strategic and International Studies. Alexander indicated the military is not alone, and that government agencies and industry also lack situational awareness. Alexander believes that "foreign governments have substantially more resources and more worrisome motives for attacking U.S. networks." The new Cyber Command is working to develop a situational awareness tool that could be shared with other government agencies and the private sector.[31]

Congress does have several cybersecurity bills currently pending. Melissa Hathaway, president of Hathaway Global Strategies and former cybersecurity official, recently conducted a study and found the nine most important pending cybersecurity bills. Data Breach Legislation (S. 139) would standardize the 46 State data breach laws, and all reporting would go to the U.S. Secret Service which could hurt information sharing efforts. The Data Accountability and Trust Act (H.R. 2221) would require ISPs to inform users when they become infected with malware, and the International Cybercrime Reporting and Cooperation Act (S. 1438 and H.R. 4692) would authorize the State Department to create a cybersecurity Ambassador. The Cybersecurity Enhancement Act (H.R. 4061) would give NIST additional responsibility and would support cyber research and development. FISMA II (S. 921) is an update to the current FISMA guidelines, which are widely seen as compliance driven, and the Intelligence Authorization Act (H.R. 2071) would strengthen Intelligence Community cybersecurity efforts. The Cybersecurity Act of 2009 (S. 773) would help to improve private sector cybersecurity through audits and industry-developed, government-backed standards. The Grid Reliability and Infrastructure Defense Act (H.R. 5026) would have the Federal Energy Regulatory Commission protect the electric transmission and distribution grid from cyber threats, and the Energy and Water Aproppriations Act 2010 (Law) give additional funds for cybersecurity and establishes a National Cyber Center for the smart grid.[32]

[29] *Cyberspace Policy Review*. (n.d.). Retrieved June 16, 2010, from WhiteHouse.gov: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[30] Bain, B. (2010, January 28). *Cybersecurity regs seen as less restrictive in the U.S.* Retrieved June 16, 2010, from Federal Computer Week: http://fcw.com/articles/2010/01/28/web-cyber-critical-infrastructure-vulnerabilities.aspx

[31] Matthews, W. (2010, June 3). *CyberCom: U.S. Lacks Online Situational Awareness*. Retrieved June 16, 2010, from Defense News: http://www.defensenews.com/story.php?i=4655216

[32] Hathaway, M. (2010, May 25). *Melissa Hathaway Names 9 Cyber Bills to Watch*. Retrieved June 16, 2010, from The New New Internet: http://www.thenewnewinternet.com/2010/05/25/melissa-hathaway-names-9-cyber-bills-to-watch/

Russia

In a recent interview with MIT's Technology Review, Vladislav Sherstuyuk, head of the Institute of Information Security Issues at Moscow State University and member of Russia's National Security Council, confirmed that Russia is developing offensive cyber capabilities. While little information is available regarding a formal Russian cyber security strategy, a report from computer security company McAfee says that Russia, the United States, China, France and Israel are all developing capabilities that will allow them to attack and cripple computer networks and critical infrastructure. Russia has also been campaigning for an international cyber arms-control agreement to stop cyber crime. Sherstuyuk said that Russia is more concerned with terrorists using the Internet for recruitment and planning attacks than cyberwar. As is the case in many countries, Russia is concerned about attribution – determining where the attacks originate.[33]

Russia is calling for an international treaty that would end the cyber arms race, and says that a treaty would prevent nations from engaging in cyber warfare. The United States argues that instead of another international institution, it would be more effective to improve collaboration with international law enforcement agencies. Declaring cyber criminal institutions and cyber attacks illegal will make military cyberattacks illegal while simultaneously engaging in international cooperation and collaboration. The 2004 Council of European Convention on Cybercrime actually already includes 22 nations, excluding Russia and China.[34]

A delegation from the United States met with Russian officials last month as part of the U.S.-Russia Information and Communication Technology (ICT) Roundtable and bilateral talks with Russia's Ministry of Communications in Moscow. Discussions focused on broadband, Internet governance, cybersecurity, spectrum management, and coordination of positions for the upcoming meetings at the International Telecommunication Union. The U.S. delegation included members from the State Department, the Federal Communications Commission, and the Commerce Department's National Telecommunications Information Administration.[35]

Some experts warn that the United States should not enter a formal arms control treaty with Russia until the Russian government agrees to crack down on its cyber crime industry. UK Serious and Organized Crime Agency e-crime chief Andy Auld says that Russian law enforcement will likely do nothing about the cyber crime problem. Auld even claims that the RBN has Russian local police, judiciary and local government "in its pocket."[36]

Although Russia has long been thought of as a haven for cyber criminals, the nation is now taking steps to crack down on cyber crime. The Russian Coordination Center, which administers Russia's domain registries (.ru), announced in April that they would verify the identities of every registrant including businesses and individuals by requiring a copy of a passport or legal registration papers.[37] Olga Ermakova, informational projects manager with the Coordination Center for the .ru top-level domain, says that the new changes will help Russia align with international best practices, and will cut down on spammers since criminals could previously register domain names under fake identities and use them to send spam or set up botnets.[38]

[33] Talbot, D. (2010, April 16). *Russia's Cyber Security Plans.* Retrieved June 10, 2010, from MIT Technology Review: http://www.technologyreview.com/blog/editors/25050/

[34] Koeppen, B. (2009, June 9). *US vs. Russia: Cyber Space Dispute.* Retrieved June 10, 2010, from The New New Internet: http://www.thenewnewinternet.com/2009/06/29/us-vs-russia-cyber-space-dispute/

[35] Bain, B. (2010, May 11). *US, Russia kick off talks on IT.* Retrieved June 10, 2010, from Federal Computer Week: http://fcw.com/articles/2010/05/11/web-u.s.-russia-it-talks.aspx

[36] Bronk, C. (2010, January 19). *Toward Cyber Arms Control with Russia .* Retrieved June 10, 2010, from World Politics Review: http://www.worldpoliticsreview.com/articles/4959/toward-cyber-arms-control-with-russia

[37] Cheek, M. (2010, March 23). *Russia to Crack Down on Cyber Crime.* Retrieved June 10, 2010, from The New New Internet: http://www.thenewnewinternet.com/2010/03/23/russia-to-crack-down-on-cyber-crime/

[38] McMillan, R. (2010, March 19). *To fight scammers, Russia cracks down on .ru domain.* Retrieved June 10, 2010, from Computer World: http://www.computerworld.com/s/article/9173778/To_fight_scammers_Russia_cracks_down_on_.ru_domain

Yevgeny Kaspersky, former Russian hacker, says that the most sophisticated attacks online come from Russia. Kaspersky says that Russian malware and design is always more complicated and technical than attacks from other parts of the world like China or Latin America. The reformed hacker believes that Russia's technical education is the reason for its abundance of hackers and the sophistication of their attacks. Kaspersky believes that there should be some form of government control of cyberspace since our economies and businesses depend on the Internet, but are unable to control it. Kaspersky recommends issuing every user an internet passport, and says that security is more important than preserving full freedom.[39]

China

Although China is usually called out as the most threatening nation online and a haven for state-sponsored cyber criminals, China has actually been taking steps to improve cybersecurity. The 2010 Q1 report from Kaspersky says that the .cn top-level domain went from hosting 32.8 percent of all malware in Q4 2009 to only 12.84 percent in Q1 2010. This is likely the result of a new Chinese policy that restricts the .cn domain to registered businesses and requires applicants to provide their business license and a government ID to the registrar. "Chinese operators are often blamed in large-scale attacks…The Chinese response has been to state that they are constantly under attack themselves and that the servers conducting the attacks are often under the control of a foreign intruder."[40]

According to the People's Daily, the official paper of the Communist Party, the Chinese government is working to toughen laws that determine how hacking crimes are handled by courts. China has also called for changes to a law on online information safety, along with additional measures that would reduce cybercrime. Last year, China released a law that requires Internet service providers to take action when a user is using a network to violate another person's civil rights. Last year, China also passed regulations to protect users from cyber data theft, and regulations that require China's telecom network operators to fight botnets and false information being used to register domain names.[41]

China has worked to increase awareness and prosecution of cyber crime. Chinese security researchers have now taken jobs working for security companies in China, which has led to claims that Chinese hackers are state-sponsored, when Chinese researchers actually work for the government to legitimize their careers. The security industry in China is still in its early stages, however, which has led to many aspiring hackers turning to crime when they do not find legitimate work. New laws in China have targeted this new generation of hackers, and a new law in 2009 made even the distribution of hacking tools a crime in China.[42]

China has made clear its intention to become a leading player in the fields of information and cyber warfare, and began publishing theories, doctrine and policies more than 20 years ago. "Since the mid 1990s the Chinese army has implemented a modernization program guided by the concept of 'informationization' (which translates as dominance over information technologies and cyberspace)."[43] The Central Military Commission Committee of the Chinese Communist Party has also endorsed the concept of 3 Warfare, which includes psychological warfare, media warfare and legal warfare. China also has several military training centers that provide cyber-war training programs. These centers and the Chinese military conduct information warfare exercises showing that China is

[39] Rainsford, S. (2010, March 11). *Inside the Mind of a Russian Hacker.* Retrieved June 10, 2010, from BBC News: http://news.bbc.co.uk/2/hi/technology/8561910.stm

[40] Moore, H. (2010, June 11). *China taking noteworthy steps to improve cybersecurity.* Retrieved June 16, 2010, from The Last Watchdog: http://lastwatchdog.com/china-noteworthy-steps-improve-cybersecurity/

[41] Fletcher, O. (2010, February 2). *China takes step to toughen hacking laws.* Retrieved June 16, 2010, from Computer World: http://www.computerworld.com/s/article/9150718/China_takes_step_to_toughen_hacking_laws

[42] Moore, H. (2010, June 11). *China taking noteworthy steps to improve cybersecurity.* Retrieved June 16, 2010, from The Last Watchdog: http://lastwatchdog.com/china-noteworthy-steps-improve-cybersecurity/

[43] Ventre, D. (2010, May 18). *China's Strategy for Information Warfare: A Focus on Energy.* Retrieved June 16, 2010, from Journal of Energy Security: http://www.ensec.org/index.php?option=com_content&view=article&id=241:critical-energy-infrastructure-security-and-chinese-cyber-threats&catid=106:energysecuritycontent0510&Itemid=361

transitioning to practicing cyber capabilities, although their information warfare and cyber warfare capabilities are still unknown.[44]

We also know that China does operate on an extensive censorship system, and blocks sites that are pornographic or subversive. Wang Chen, chief of the Cabinet's Information Office, says that the Chinese government will soon begin to crack down on online information from international sources in an effort to stop online gambling, fraud, and activist sites that are undermining communist rule. Wang said that China "will strengthen the blocking of harmful information from outside China to prevent harmful information from being disseminated in China and withstand online penetration by overseas hostile forces." Last month, China strengthened a law that requires telecommunications and Internet companies to inform on users that discuss state secrets, and in February, the Chinese government announced that anyone wanting to operate a website must meet with regulators in person and provide photos of themselves.[45]

The Chinese government also enforces the infamous "Golden Shield" which is a filter that blocks politically sensitive material from entering or leaving China. In the West, the information block is referred to as the "Great Firewall of China," but this shield may give China an advantage in a future cyberwar. Jody Westby, chief executive of security consultancy Global Cyber Risk, says that the government control over information and its tight relationship with Internet service providers could help China better coordinate a defense against online attacks. Westby explains that in the U.S., the autonomy of the Internet could leave it vulnerable to state-sponsored enemies stealing classified information or shutting down critical servers. Jason Street, a consultant for Stratagem 1 Solutions, says that if China ever did use viruses as a military tool, it could use the Golden Shield to prevent collateral damage. Marcus Ranum, chief security officer of Tenable Security, says that China could also use an Internet kill switch to completely isolate the Chinese Internet in case of a cyber-war. The United States has no such option, since the Internet in the U.S. is less regulated and considered a basic freedom.[46]

A recent report from Symantec MessageLabs found that 28.2 percent of malicious emails targeting corporations came from China, either from Chinese individuals or computers in China that were under the control of a botnet.[47] U.S. Navy Admiral Robert Willard recently appeared before the U.S. House Armed Services Committee and warned that attacks from within the People's Republic of China are targeting U.S. military and government networks. Willard said that "these threats challenge our ability to operate freely in the cyber commons, which in turn challenges our ability to conduct operations during peacetime and in times of crisis."[48]

United Nations

Experts all seem to agree that the international community needs some organization that can provide risk advisories on cyber threats and also respond to attacks against government. The U.S. Cyber Consequences Unit (US-CCU), an independent, nonprofit research institute, recently studied the cyberattacks against Georgia in 2008, and said that cyber incidents will likely be a part of future conflicts. John Bumgarner, the principal author of the study and US-CCU's research director for security technology, says there is a need for an international organization that can foster the relationship between nations and hold international discussions about cyber attacks and

[44] Ventre, D. (2010, May 18). *China's Strategy for Information Warfare: A Focus on Energy.* Retrieved June 16, 2010, from Journal of Energy Security: http://www.ensec.org/index.php?option=com_content&view=article&id=241:critical-energy-infrastructure-security-and-chinese-cyber-threats&catid=106:energysecuritycontent0510&Itemid=361

[45] *China Targets 'Foreign Forces' in Web Crackdown.* (2010, May 4). Retrieved June 16, 2010, from NewsFactor.com: http://www.newsfactor.com/story.xhtml?story_id=73102

[46] Greenberg, A. (2007, July 31). *China's Golden Cyber-Shield.* Retrieved June 16, 2010, from Forbes: http://www.forbes.com/2007/07/30/china-cybercrime-war-tech-cx_ag_0730internet.html

[47] Higgins, K. J. (2010, March 25). *Report: Most Targeted Attacks Originate From China.* Retrieved June 16, 2010, from Dark Reading: http://www.darkreading.com/insiderthreat/security/attacks/showArticle.jhtml?articleID=224200336

[48] Thibodeau, P. (2010, March 26). *Military warns of 'increasingly active' cyber-threat from China.* Retrieved June 16, 2010, from Computer World: http://www.computerworld.com/s/article/9174242/Military_warns_of_increasingly_active_cyber_threat_from_China_

warfare. Bumgarner points out that we do not even have internationally agreed-upon definitions of cyber conflicts and that the problem of attribution makes it difficult to use deterrence as a strategy. Perhaps a U.N. cybersecurity council could fill the gap in improving international collaboration and discussion.[49]

International Telecommunications Union Secretary General Hamadoun Toure spoke at a World Economic Forum debate earlier this year, and said that the risk of cyber conflict is increasing, and that nations must come together and form a treaty that would stop countries from launching offensive cyber strikes. The UN official said that the framework for such a treaty would include the agreement that countries will protect their citizens and their right to access to information, as well as an agreement not to harbor cyber terrorists.[50]

Russia is strongly encouraging a UN cybersecurity treaty which is popular among developing countries who want to have influence over international cyber law. The United States and the UK, however, back the Budapest Convention on Cyber Crime, and fear that UN negotiations would derail progress on legislation that has been made around the world based on the Budapest model. Prosecutors currently rely on the Budapest Convention to secure electronic evidence against criminals across borders.[51]

NATO

Brig. Gen. Norbert Stier with NATO Headquarters explains that NATO has always been based on its ability to provide collective defense, crisis management and conflict resolution. Stier says that member nations must provide information to share with other members, and that NATO must provide communications and information systems support.[52] Experts at a NATO workshop in Brussels, Belgium, last October said that the complex policy, legal and governance issues that come with creating a single interoperability level is a bigger challenge than developing collaboration and information sharing capabilities. Dag Wilhelmsen, technical director of the NATO Communication and Information Systems Services Agency, says that NATO must create a common language and vision for cybersecurity. NATO must determine what information can be shared between nations, and what level of trust can be given to non-member nations. NATO must also create a common definition for cybersecurity that all nations can use while discussing governance and policy challenges.[53]

NATO is reportedly now considering the use of military force against nations who launch cyber attacks against member states. A team of NATO experts, led by Madeline Albright, said an attack that targeted the critical infrastructure of a NATO country could be considered an armed attack, justifying retaliation. The group also said that an attack that targeted NATO's command and control systems or energy grids could lead to defensive measures being taken under article 5, which says that an attack against one NATO state is an attack against them all. NATO heads of government will meet in Lisbon in November to discuss the use of military force in response to cyber attacks.[54]

Albright's group recently released a report of recommendations for what NATO could keep in mind while developing their new strategic concept in November. The report discusses whether or not a cyber attack violates

[49] Bain, B., & Beizer, D. (2009, August 21). *Do we need a U.N. cybersecurity council?* Retrieved June 10, 2010, from Federal Computer Week: http://fcw.com/Articles/2009/08/24/WEEK-International-cyber-attack-fears.aspx?Page=1

[50] *UN agency calls for global cyberwarfare treaty, 'driver's license' for Web users.* (2010, January 31). Retrieved June 10, 2010, from Prison Planet: http://www.prisonplanet.com/un-agency-calls-for-global-cyberwarfare-treaty-'driver's-license'-for-web-users.html

[51] Ballard, M. (2010, April 15). *Conflict over proposed United Nations cybercrime treaty.* Retrieved June 10, 2010, from Computer Weekly: http://www.computerweekly.com/Articles/2010/04/15/240914/conflict-over-proposed-united-nations-cybercrime-treaty.htm

[52] Mowery, B. (2010, January 2). *NATO Nations Embrace Collaboration Technologies, Seek Security Solutions.* Retrieved June 10, 2010, from AFCEA Signal Magazine: http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=2154&zoneid=8

[53] Mowery, B. (2010, January 2). *Bringing Security to NATO's Front Lines Requires Policy, Governance and Legal Action.* Retrieved June 10, 2010, from AFCEA Signal Magazine: http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=2155&zoneid=8

[54] Smith, M., & Warren, P. (2010, June 6). *Nato warns of strike against cyber attackers.* Retrieved June 10, 2010, from The Sunday Times: http://www.timesonline.co.uk/tol/news/world/article7144856.ece

Article 5 of NATO's treaty, and whether a significantly damaging cyber attack could warrant physical consequences.[55]

At the AFCEA West 2010 conference in San Diego last February, Adm. James Stavridis, NATO's supreme allied commander Europe and the U.S. European Command commander, said that he believes future attacks against NATO nations will increase, and that NATO must define what constitutes an attack in cyberspace. Stavridis also said that NATO should face cyber issues by launching new ideas and technologies instead of weapons. NATO has taken the first step in facilitating international cyber cooperation by setting up the Cooperative Cyber Defense Center of Excellence in Estonia.[56] The Cyber Defense Center works to research cyber war techniques and incidents, and coordinates efforts with other NATO members to create cyber war defenses and offensive weapons. A recent agreement between Estonia and NATO is a result of that research, which has also helped to raise awareness among NATO nations. NATO has signed similar agreements with Slovakia, Turkey, Britain and the United States.[57]

[55] Perera, D. (2010, May 17). *NATO grapples with cyber attack response.* Retrieved June 10, 2010, from Fierce Government IT: http://www.fiercegovernmentit.com/story/nato-grapples-cyber-attack-response/2010-05-17

[56] Rosenberg, B. (2010, April 6). *NATO unites to thwart cyber threats.* Retrieved June 10, 2010, from Defense Systems: http://defensesystems.com/articles/2010/04/06/cyber-defense-nato.aspx

[57] *The NATO Cyber War Agreement.* (2010, May 1). Retrieved June 10, 2010, from Strategy page: http://www.strategypage.com/htmw/htiw/articles/20100501.aspx