

Toward a Closer Digital Alliance

Melissa E. Hathaway

Countries will need to reconcile the facts that their Internet infrastructures are vulnerable and less resilient to attack and that their economic dependence on the Internet makes cooperation between countries on cybersecurity issues essential. Disparate and uncoordinated cyber defense schemes could adversely affect individual and collective security, privacy, usability, transparency, speed, and interoperability. Much tighter alignment and better integration of European and NATO initiatives with national laws, policies, and funding priorities is necessary to counteract threats against national networks and infrastructure. Only through international cooperation and private-public partnerships can cyber defense measures succeed.

Introduction

The next ten years will be a period of transition, in which countries will need to reconcile the facts that their Internet infrastructures are vulnerable and less resilient to attack and that their economic dependence on the Internet will not permit them to abandon the path they are on. The Internet has connected every nation and nearly all essential services, and has blurred the line between sovereign assets and commercial space. This digital entanglement of private and public infrastructure also makes it difficult to draw a distinction between military and civilian systems and property. In May 2010 two important strategy documents were introduced that bring this dilemma into focus.

The next ten years will be a period of transition, in which countries will need to reconcile the facts that their Internet infrastructures are vulnerable and less resilient to attack and that their economic dependence on the Internet will not permit them to abandon the path they are on.

On 19 May 2010, the European Commission published its Communication on a European Digital Agenda,¹ just two days after a group of experts published its analysis and recommendations on a new strategic concept

Melissa Hathaway led President Obama's Cyberspace Policy Review and previously led the development of the Comprehensive National Cybersecurity Initiative (CNCI) for President George W. Bush. She is now President of Hathaway Global Strategies LLC and Senior Advisor at Harvard Kennedy School's Belfer Center.

for the North Atlantic Treaty Organization (NATO) entitled NATO 2020: Assured Security; Dynamic Engagement.² These two documents articulate the need to harmonize information communications and technology (ICT) initiatives and align each nation's security and economic interests to promote, among other things, greater digital interoperability, enhanced Internet trust and security, faster Internet access (broadband), and increased focus and funding for research and development (R&D). These two documents also detail the importance of nations providing, when appropriate, mutual assistance through better information sharing and undertaking crisis response operations within, along, and beyond their respective borders. These are important goals to reach for. However, they likely are not attainable without much tighter alignment and better integration of European and NATO initiatives with national laws, policies, and funding priorities.

The cross-border flow of goods, services, people, technology, ideas and information is being limited by those who would exploit these channels to commit crime and provoke conflict. Nations need to recognize that while the goals of these disruptive forces may vary (exploitation of children, propagation of extremist messages to recruit terrorists, or electronic crime for example) the means being used are the same. Moreover, these activities are being carried out using the public infrastructure, distributing "goods" such malware or botnet and services like extortion, espionage, money raising, message distribution, and mobilization with broad anonymity. Governments organize by mission—defense of the homeland, prevention and mitigation of crime, critical infrastructure protection—and are therefore sub-optimized for well-coordinated and comprehensive counter-responses. Often, defensive strategies developed in one mission area are not shared with other missions and thus lower a country's overall security and generate uncertainty in online transactions. The trust that has enabled the Internet to grow is being challenged with every transaction. And while some may argue that the government must take charge in restoring that trust, achieving success in this arena requires stronger reliance on the private sector. We must

Information infrastructure has become valuable to society over and above its value to the corporations that own and control it. The residual value must be secured by the public, either through laws, policies, taxes, procurement incentives (discounting), regulations, liabilities, subsidies or other market levers.

operationalize the private-public partnership to better understand the nature of the problem and empower the private sector to help secure our national networks and infrastructures.

Are all countries on a consistent path?

In order to realize a new international security framework by 2020, built upon a digital agenda, Europe and NATO must effectively

align government (public) and corporate (private) interests. Information infrastructure has become valuable to society over and above its value to the corporations that own and control it. The residual value must be secured by the public, either through laws, policies, taxes, procurement incentives (discounting), regulations, liabilities, subsidies or other market levers. For this reason, nations must begin a dialogue on how to conceive and execute a strategy that embodies multilateral security values and protects the interests of all parties.

The United States, United Kingdom, France, and Germany often lead Europe and NATO in the adoption of such broad based reform agendas. However, because some alliance partners have different priorities in defending against the threat, it is difficult for them to come together around a common, collective European or NATO vision. For example, Germany has determined that botnet (large clusters of zombie computers, controlled by third parties, that can be used for cyber attacks) infestation of its private (citizen or corporate) infrastructure is a priority for national defense. As such, the German Federal Office for Information Security (BSI) has required the cooperation of its Internet service providers (ISPs) in tracking down infected machines and providing advice to users on how to clean their computers.³ On the other hand, the United Kingdom has determined that data breaches caused by crime and espionage are its highest priority, and they have chosen a different path. In April 2010, the U.K. parliament approved the United Kingdom Data Protection Act that imposes a £500,000 financial penalty when the Information Commissioner determines there has been a serious contravention of data protection principles.⁴ In other words, if a corporation has not implemented adequate defenses of its networks or information assets and a breach occurs (illegal copying or movement of data, for example), it could be subject to the fine.

Conversely, the United States and France have determined that the defense of their military and government networks are of the highest priority. France has established the French Network and Information Security Agency (FNISA) and has charged it with the mission of continuous surveillance of sensitive government networks as well as the implementation of appropriate defense mechanisms.⁵ Because the boundaries between government and private sector networks are blurred, the United States is struggling to define the role of government in protecting private sector networks and infrastructure. Meanwhile, the United States has issued requests to industry (a notice of inquiry) seeking public comment on the proposed creation of a voluntary cybersecurity certification program through which participating communications service providers would be certified—by the Federal Communications Commission (FCC) or an approved third party—as adhering to a set of cybersecurity objectives and practices.⁶ This may result in an approach similar to Germany's, where the United States relies more on the ISP's to provide dynamic defense capabilities along with commercial Internet, network, and other communications services.

In stark contrast, the Netherlands, Italy, Sweden and other European nations are developing cybersecurity approaches that appear to better align

with NATO's initiatives and the Digital Agenda. As individual nations implement different laws, polices and regulations it is clear that most countries are not following a consistent path toward achieving the stated vision. In fact, their pursuits may make it more difficult to share information or cooperate in a time of crisis. It cannot be ignored that a cybersecurity failure in one nation may impact the entire alliance and therefore a transnational framework must be developed and tracked so that each nation can be witting of how their internal laws, regulations, and policies may affect their ability to fulfill broader regional and security treaty commitments.

**Who is responsible for mutual assistance,
information sharing and assured Survivability?**

The NATO Group of Experts report recognizes the world's increased reliance on potentially vulnerable information systems and recommends that the alliance be able to "contribute to the broader security of the entire Euro-Atlantic region. Just as a homeowner has an interest in the safety of his or her neighborhood, so NATO has reason to be concerned about stability throughout the region of which it is a part."⁷ However, what is NATO's role to be in a situation where the policies, technologies, and expertise needed to ensure security reside in civilian and private holdings and not in the military's area of influence? How are areas of common concern defined and information shared prior to a time of crisis, when the knowledge resides in private corporations? The entanglement of private and public infrastructure has made it difficult to draw a distinction between private and public property.

As more of industry moves its services to an Internet based infrastructure, one could envision a digital crisis similar to the ash clouds over Iceland that halted air traffic around the world for days earlier this year. What if, for example, the e-ticketing of several major airlines and train systems were taken

As more of industry moves its services to an Internet based infrastructure, one could envision a digital crisis similar to the ash clouds over Iceland that halted air traffic around the world for days earlier this year.

off-line. What mechanisms exist to ensure that service can continue, passengers could be tracked, and packages moved? This is not an impossible hypothetical, as a reservation systems breakdown for United Airlines stranded thousands of passengers and disrupted flights around

the United States in January 2006. Additionally, governments around the world have already catalogued tens of thousands of reported vulnerabilities in today's power grid. While regulation may force compliance with specific rules, the shift from isolated systems to open protocols makes it possible for outsiders to gain access to remote sites through the use of modems, wire-

less connections, and the Internet. While not seen to date, the future holds the possibility that the electric power grid could be susceptible to denial of service attacks through networked devices like routers and meters that have designated public IP addresses.⁸ If this were to occur it would result in loss of communication between the utility and meters—and the subsequent denial of power to private and public institutions alike. Would NATO’s crisis response capability under Article 4 improve the situation in either of these scenarios? Perhaps not, as Article 4 is a consultation and information sharing arrangement that activates when a member nation perceives its territorial integrity, political independence, or security is threatened.⁹ What NATO can do, however, is identify areas of common concern among nations and identify what expertise could be leveraged from the private sector as it pursues the goals of the Digital Agenda.

Initiatives in Europe and the United States have sought faster broadband Internet access for every citizen, to fully support our information society and global e-commerce. For example, Finland passed a law this year stating that every one of its citizens will have the right to access one megabit per second (Mbps) broadband connection. The United Kingdom promises to have a minimum connection of 2 Mbps to all homes by 2012. Similarly, the United States promises to wire more Americans with much faster Internet connections but acknowledges that more broadband would increase security vulnerabilities.

The FCC noted that the country “needs a clear strategy for securing the vital communications networks upon which critical infrastructure and public safety communications rely.”¹⁰ Key

Key in this debate is whether countries regulate broadband Internet and classify it as a telecommunications service, which of course is quite a contentious issue in the United States today.

in this debate is whether countries regulate broadband Internet and classify it as a telecommunications service, which of course is quite a contentious issue in the United States today.

Regulation at this stage might be important in order to assure communications reliability and resilience. This is critical because as the communications infrastructure migrates from older to newer technologies, services will be carried over a communications network that may or may not be built to the same standards that the traditional voice telephone system was built for. Government essential services like energy and public safety that rely on an Internet backbone could be put at risk. As we embrace broadband, it will be equally important for the alliance to gain a better understanding of the reliability and resiliency standards required for our collective security posture.

This may be addressed in the components of the Digital Agenda that call for enhanced Internet trust, access, and security, and greater digital interoperability. The coming years will bring about rapid, if uneven, changes

in networked computers and systems. Broadband deployment and adoption will improve Internet access and speed, but it will also increase the speed and velocity of the delivery of malware as well as the ability of organized crime or rogue states to access and exploit our networks—something no country or company is completely prepared for.

These challenges can be expected to intensify with the rapid adoption of cloud computing to cut IT costs, increase efficiencies, and enable greater government-wide collaboration and data exchange. According to the National Institute of Standards and Technology (NIST), “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”¹¹ Cloud computing and virtualization technologies offer many benefits and may even displace the desktop computer. But with those benefits come potential information security and assurance pitfalls, as well as law enforcement and legal issues. Wherever data is stored, it falls under the legal paradigm of that country. That includes the privacy laws. The United States does not have a single federal, government-wide data-breach law. Therefore, if your data is in California or Massachusetts, it is held under a different set of privacy notification laws than in Texas or Florida. This is similar to Europe. If the data is stored in Germany, it falls under a different set of laws than in Estonia, Denmark, or the United Kingdom.

Why is this important? In 2009, hundreds of companies fell victim to “Operation Aurora,” a coordinated attack targeting and illegally copying their intellectual property.¹² Many companies experienced a significant breach; companies in the United Kingdom may be subject to an investigation by the Information Commissioner and subject to a £500,000 financial penalty when similar attacks occur in the future. Even if the initial damage does not result in massive economic costs, attacks like Operation Aurora highlight the need for development of cooperation procedures between law enforcement agencies, computer emergency response teams (CERT’s) as well as ISP’s and the IT industry. Insecure cloud implementation could allow an attacker to rapidly provision large quantities of resources that can be leveraged for malicious use. Due to the speed with which this can occur, the attacker effectively has the ability to rapidly provision attack platforms such as botnets and then just as quickly remove them and destroy the evidence. If attacks are not detected and stopped while in process, the only evidence may be when the owner of the environment gets the bill for the large resource utilization or a visit from law enforcement. For example, hundreds of Apple’s iTunes customers recently fell victim to a fraudulent scam for songs, videos, and applications. The security incident was not detected by the company; instead, customers reported the problem when they noticed excessive charges on their credit cards for purchases they had not made.¹³

The Council of Europe Convention on Cybercrime recognizes the need for cooperation between the private and public sectors, and signatories to the convention have agreed that “security and the protection of rights is the

responsibility of both public authorities and private sector organizations.”¹⁴ However, “information sharing across borders is still not as good as it needs to be” according to Patrick Pailloux, General Director of the French Network Information Security Agency.¹⁵ The alliance must create the venue in which information sharing and learning can be improved. No single forum exists to facilitate this information sharing. Rather, constructs exist on an *ad hoc* basis, reflecting the disparate missions within each member country, including but not limited to defense of the homeland, crime prevention, critical infrastructure protection, and consumer protection.

To effectively defend the information infrastructure requires that private and public parties identify threats quickly and mitigate their impact effectively. Across the

IT industry, threats and vulnerabilities have traditionally been handled by individual companies, and companies have responded to those threats individually. This is similar to how nations address the problem. Illicit and illegal ac-

To effectively defend the information infrastructure requires that private and public parties identify threats quickly and mitigate their impact effectively.

tivities ignore national boundaries, ignore private-public distinctions, and leverage the public infrastructure (Internet, Cloud, Broadband) to exploit its vulnerabilities. Therefore, it is imperative that the alliance look at the policies and laws, like the ones cited above, that may disrupt or destabilize cross-border information sharing and assistance. There is a need for cooperative approaches towards gathering electronic evidence, prioritizing jurisdiction, enlisting private sector talent, and perhaps conscripting the ISP’s to shoulder a broader burden. Further, there is a need to update the data protection regulatory framework on both sides of the Atlantic in order to address concerns arising from globalization and new technologies, and the need to protect citizens’ right to privacy in the digital environment.

Is there consensus on what constitutes an act of aggression in cyberspace?

NATO’s cyber defense policy was endorsed at the Bucharest Summit in April 2008 and was driven in large part by Estonia’s request for emergency assistance from NATO for the defense of its digital assets in connection with a coordinated distributed denial of service (DDoS) in 2007. Estonia did receive help; however, its call for assistance highlighted gaps in NATO’s policies for the digital world. The attacks against Estonia caused a debate regarding what constitutes an act of aggression in cyberspace. Many felt that the attacks against Estonia were not serious enough to constitute an armed attack and thus activate Article 5, under which an attack on any member is considered to be an attack on all member states. Further, because the conscripted computers and botnets that were conducting the DDoS were

internationally distributed, it was not possible to attribute responsibility to any one nation. This of course frustrates response doctrine and execution, and makes the principle of proportional response difficult.

The use of civilian infrastructure for military or hostile means also challenges the traditional distinction between combatants and noncombatants. For example, if a home computer has been hijacked and is used for an assault on a country, like Estonia, is that home or citizen now a combatant? If the hacker was hired by a government to perform this deed, but he is not wearing a uniform, is he a combatant? It also confounds military concepts and treaties regarding legal sanctuary and neutrality. For example, in July 2009 the United States and South Korea fell victim to a DDoS attack against thousands of computers and major government, media, and financial websites. The attacks were launched from at least five different control hosts in multiple countries including the United States. The government turned to industry to determine the origin and character of the threat and asked the ISP's to shut down the operations and restore services. If any of these attacks had been launched from a hospital or school, it may not have been as easy to stop the attacks. Furthermore, these types of events highlight governments' dependence on industry to provide assistance in times of crisis.

These primitive assaults on public and private institutions highlight the lack of precedent to guide international action on cyberspace intrusions. Estonia's defense minister, Jaak Aaviksoo, called for the development of a stronger capability to respond to cyber attacks and demanded the issue receive serious discussion and information exchange.¹⁶ The Cyber Defense Management Authority in Brussels continues to work on guidance and standards by which the alliance could determine its responsibility to provide assistance in situations such as these. However, what may be needed is a more thoughtful discussion and transnational approach to infrastructure protection, one that minimizes the dangers of attack and is inclusive of the private entities that will likely be called upon to take action against the perpetrators.

Aligning the strategy with execution

The above scenarios highlight the need to align cybersecurity initiatives with future research and development priorities, especially in the face of strained economic forecasts and flat-lined IT budgets. Accordingly, the alliance must jointly explore technology development including enhanced commercial-off-the-shelf product development, through joint planning and investment. Collectively, there is a need for an infrastructure that is Internet based and that allows us to live and work online with confidence. The vision must close the gap of infrastructure insecurity and attacker capabilities and make the Internet a safer place.

The European Commission's Programme Framework-7 (FP-7) has allocated €1.4 billion for proposals in security research to drive the innovation agenda. One of the evaluation criteria for this investment is transnational cooperation among companies and solutions that meet pan-European

needs. Objectives include restoring security and safety in case of a crisis; improving security systems integration, interconnectivity, and interoperability; and increasing the security of infrastructure and utilities. Similarly, the United States has the National Information Technology and Research and Development (NITRD) process that prioritizes, coordinates, and funds a four billion dollar annual IT research agenda that promotes infrastructure improvements and improves the trust and integrity of online transactions among other security initiatives. The alliance would benefit from a strategic agenda of intellectual “federalization” where countries work to ensure a seamless and effective research partnership informed by common security priorities and jointly pursued by academic institutions, small businesses, and multi-national companies.

Moreover, the alliance should leverage its members’ participation in regional or other forums to promote common policy objectives, focus the work of existing international organizations, and limit duplication of effort among them. More than a dozen international organizations—including the United Nations, the Group of Eight, the Organization for Security and Co-operation in Europe, NATO, the Council of Europe, the Asia-Pacific Economic Cooperation forum, the Organization of American States, the Organization for Economic Cooperation and Development, the International Telecommunications Union, and the International Organization for Standardization—address issues concerning the information and communications infrastructure. New organizations are beginning to consider cybersecurity policies and activities, while others are expanding the scope of their existing work. These venues consider policies and conduct activities that sometimes conflict and often overlap.

The agreements, standards, or practices that these organizations promulgate have global effects and cannot be ignored. The Digital Agenda does not explicitly refer to the systematic promotion of open standards and interoperable IT systems as a means to encourage innovation and improve cost effectiveness, but it

does suggest using the full range of “relevant standards when procuring hardware, software and IT services, for example by selecting standards which can be implemented by all interested suppliers,

. . . the alliance needs to promulgate its vision into the other policymaking venues and begin to centralize and focus the discussion around what is needed for all nations.

allowing for more competition and reduced risk of lock-in.”¹⁷ If the alliance continues to work in its agreed upon framework for evaluating information security products, which allows products evaluated in one country to be recognized and certified by customers in another country, all nations would be better off. Additionally, there is a need to strengthen this framework and add to its requirements for enhanced product assurance, interoperability testing, and security effectiveness testing, and to potentially develop and

agree on an international standard for supply chain-of-custody. Finally, the alliance needs to promulgate its vision into the other policymaking venues and begin to centralize and focus the discussion around what is needed for all nations.

Conclusion

The member nations of the EU and NATO are pursuing individual paths, adopting technology at different rates, and mitigating risk with different policy and legal levers. Many of the initiatives that are underway today,

Many of the initiatives that are underway today, although clearly well intentioned and focused on addressing near-term priorities, nonetheless may have the long term effect of facilitating the disruption or destabilization of cross-border modernization initiatives.

although clearly well intentioned and focused on addressing near-term priorities, nonetheless may have the long term effect of facilitating the disruption or destabilization of cross-border modernization initiatives. What is sorely needed is a coordinated and collabora-

tive approach to the growing problem, one that provides for appropriate information sharing and mutual assistance obligations governed by regional policies and treaties. These two important 2020 strategy documents are a starting point and appropriately note that it will take at least a decade to realize their respective visions. And while it will take time to achieve progress towards these visions, we also must recognize that no one country can achieve them alone. The future is bright and technological innovations that will empower and improve lives should not be feared. But if not approached thoughtfully, through international cooperation and private-public partnerships, disparate and uncoordinated cyber defense schemes could adversely affect individual and collective security, privacy, usability, transparency, speed, and interoperability.¹⁸

Notes

¹ Digital Agenda Europe contains following focus areas: (1) Create a single digital market; (2) Promote greater digital interoperability; (3) Boost Internet trust, access, and security; (4) Enable much faster Internet access (broadband); (5) Increase focus and funding for R&D; (6) Enhance digital literacy and inclusion; (7) Evaluate how ICT can be used to address climate change and aging population. European Union, *Europe 2020: A European Strategy for Smart, Sustainable, and Inclusive Growth*, May 2010, <http://ec.europa.eu/eu2020/pdf/COMPLETE%20EN%20BARROSO%20%20%20007%20-%20Europe%202020%20-%20EN%20version.pdf>.

² North Atlantic Treaty Organization, *NATO 2020: Assured Security; Dynamic Engagement. Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO*. May 17, 2010, <http://www.nato.int/strategic-concept/expertsreport.pdf>.

³ John Leyden, "German ISPs Team Up with Gov Agency to Clean Up Malware," *The Register*,

December 9, 2009.

⁴ Field Fisher Waterhouse, *Security Matters: New Financial Year, New Financial Penalty*, April 6, 2010, <http://www.fffw.com/publications/all/alerts/security-matters-penalty.aspx>.

⁵ Republic of France, The French Network and Information Security Agency (FNISA), Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) created on July 7, 2009, Press Release.

⁶ The Federal Communications Commission (FCC), *Notice of Inquiry (NOI)*, April 21, 2010.

⁷ NATO 2020: *Assured Security; Dynamic Engagement*, 19.

⁸ C4-Security Public Paper: *The Dark Side of the Smart Grid - Smart Meters (in)Security*, 2009, [http://www.c4-security.com/The%20Dark%20Side%20of%20the%20Smart%20Grid%20-%20Smart%20Meters%20\(in\)Security.pdf](http://www.c4-security.com/The%20Dark%20Side%20of%20the%20Smart%20Grid%20-%20Smart%20Meters%20(in)Security.pdf).

⁹ North Atlantic Treaty Organization, *The North Atlantic Treaty*, April 4, 1949. http://www.nato.int/cps/en/natolive/official_texts_17120.htm.

¹⁰ The United States Federal Communications Commission, *Connecting America: The National Broadband Plan*, March 16, 2010.

¹¹ Peter Mell and Tim Grance, *National Institute of Standards and Technology: Definition of Cloud Computing, Version 15*, October 7, 2009, <http://csrc.nist.gov/groups/SNS/cloud-computing/>.

¹² H.B. Gary, *Operation Aurora*, February 10, 2010, http://www.hbgary.com/wp-content/themes/blackhat/images/hbgthreatreport_aurora.pdf.

¹³ Joseph Menn, "Apple Bans Apps After iTunes Breach," *Financial Times*, July 7, 2010, <http://www.ft.com/cms/s/0/71bf6d6e-894c-11df-8ecd-00144feab49a.html>.

¹⁴ Council of Europe, "Octopus Interface Conference--Cooperation Against Cybercrime," March 23-25, 2010, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/2079_IF10_messages_1p%20key%20prov%20_26%20mar%2010_.pdf.

¹⁵ Warwick Ashford, "RSA 2010: Countries Must Work Together or Fail on Cyber Security," *ComputerWeekly.com*, March 4, 2010, <http://www.computerweekly.com/Articles/2010/03/04/240497/RSA-2010-Countries-must-work-together-or-fail-on-cyber.htm>.

¹⁶ Jeremy Kirk, "Estonia Recovers from Massive DDoS Attack," *Computerworld.com*, May 17, 2007, http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack.

¹⁷ European Commission, *Digital Agenda for Europe: What Would it Do for Me?*, May 19, 2010, <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/199&format=HTML&aged=0&language=EN&guiLanguage=en>.

¹⁸ Walter Baer, et. al., "Machiavelli Confronts 21st Century Digital Technology: Democracy in a Network Society," *An Overview of the Dagstuhl Seminar on Democracy in a Network Society, Working Paper*, Oxford Internet Institute, University of Oxford, December 10, 2009. p.17, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1521222.