Information Technology Industry Council

Comments on
"Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace" (Issued February 7, 2013)
May 21, 2013

Introduction

The Information Technology Industry Council (ITI) appreciates the opportunity to provide our reactions and suggestions regarding the "Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace" (herein Communication) released on February 7, 2013 by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy (High Representative).

ITI is a voice, advocate, and thought leader for the global information and communications technology (ICT) industry. ITI's members[1] comprise the world's leading technology companies, with headquarters worldwide. Cybersecurity is rightly a priority for all governments. The ICT industry shares the goal with governments of improving cybersecurity, and therefore our interests are fundamentally aligned in this area. As both producers and users of cybersecurity products and services, ITI's members have extensive experience working with governments around the world on cybersecurity policy. Further, our members are global companies located in various countries. Most service the global market and have complex supply chains in which products are developed, made, and assembled in multiple countries across the world. As a result, our members understand the impact of international policies on security innovation and the need for governments' policies to be globally compatible.

ITI commends the European Commission and the EU's High Representative for undertaking the challenging task of seeking to improve cybersecurity in Europe. Policymakers globally are intensely working on cybersecurity policies and laws in recognition of the evolving challenges to security in cyberspace. Throughout all of these efforts, ITI works closely and consistently with policymakers, providing substantive input and ideas and helping them to better understand the most effective approaches to improving cybersecurity.

ITI's views on the Communication are based on 1) our *Cybersecurity Principles for Industry and Government*[2] and 2) the *Global Information and Communications Technology (ICT) Industry Statement: Recommended Government Approaches to Cybersecurity*[3] co-authored by ITI, DIGITALEUROPE, and the Japanese Electronics & Information Technology Industry Association (JEITA). Both documents are important markers for successful cybersecurity policy and we are pleased that many proposed actions put forth in the Communication align with them. These include proposals to 1) develop strong national cyber resilience capabilities, 2) launch awareness and educational outreach efforts about steps all stakeholders can take to increase cybersecurity, 3) address cyber crimes and cyber criminals, 4) foster research and development

[1] See attached list of ITI member companies.
[2] http://www.itic.org/dotAsset/191e377f-b458-4e3d-aced-e856a9b3aebe.pdf
[3] http://www.itic.org/dotAsset/51ad6069-9f1b-4505-b2ff-b03140484586.pdf

(R&D) investments and innovation, and 5) establish a coherent international cyberspace policy. Underpinning many of these proposals is a very important and welcome emphasis on public-private partnerships, which we agree is the best way to improve cybersecurity.

At the same time, we believe certain proposed actions in the Communication, if not revised or implemented carefully, would decrease, not increase, security. These include proposals to 1) promote a single market for cybersecurity products, that could include Europe-specific standards, 2) require vendors to inform authorities about detected vulnerabilities, 3) have governments promote security labels or kite marks, and 4) use government purchasing power to increase cybersecurity. An underlying worrisome theme appears to be an assumption that products made in Europe are "more secure." In the following pages, we provide more details on our positions. In the cases where we have concerns, we describe how alternative approaches would significantly strengthen Europe's cybersecurity. We hope these are taken into consideration as the European Council refines its draft conclusions on the Communication, and as the Commission, Member States, and other stakeholders commence activities in these areas.

ITI also will provide, no later than June 2013, separate, detailed comments on the proposed Directive on Network and Information Security (NIS). We are very concerned with some of the approaches in the proposed Directive, including 1) an overly broad scope of what is considered critical infrastructure at greatest risk due to a cyber incident, and therefore deserving of certain obligations, 2) a proposed incident reporting framework that is top-down and unidirectional (industry to government), when a bidirectional, voluntary approach would be more effective to understanding threats and improving incident response, 3) a static, "check-the box" compliance regime, and 4) proposals to draft and use new EU-specific security standards. Businesses must adapt their risk management strategies faster than any regulatory process can move. There is a very real risk that a static compliance approach will encourage some firms to invest only in meeting requirements that are outmoded before they can even be published. A one-size-fits-all approach also could divert scarce security resources away from areas requiring greater investment towards areas with lower priority. These outcomes would not improve Europe's collective security, because the current cyber-threat environment evolves in real time and requires a complex and layered approach to security that varies greatly across industry sectors. It is imperative that the Commission seek to establish within the EU a globally compatible approach to cybersecurity policy that balances cybersecurity, innovation, and global trade.

Specific comments on Communication

The Communication includes a number of proposed actions to be taken by the Commission, European Parliament and Council, Member States, European Network and Information Security Agency (ENISA), and industry. These proposed actions fall under five strategic priorities:

- Achieving cyber resilience (2.1)
- Drastically reducing cybercrime (2.2)
- Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP) (2.3)
- Developing the industrial and technological resources for cybersecurity (2.4)
- Establishing a coherent international cyberspace policy for the European Union and promoting core EU values (2.5)

Overall, we commend nearly all of the proposed actions in sections 2.1, 2.2, and 2.5. We are concerned that many of the assumptions and proposals in section 2.4, however, will lead to decreased security. Below we provide detailed comments on these four sections. We have no comments on section 2.3.

2.1: Achieving cyber resilience

We commend the majority of the proposed actions in this section, as described below. However, we have concerns with one key proposed action: the Proposed Directive on Network and Information Security (NIS). ITI will separately provide comments on the Proposed Directive.

Proposed actions related to resilience (pp. 7-8). We concur with most of these recommendations, such as the proposals to develop strong national cyber resilience capabilities, conduct pan-European cyber incident exercises, and launch projects to fight botnets and malware. ITI companies work in partnership with many governments globally on such activities and we would be pleased to work in partnership with the Commission and Member States as you commence and strengthen work in these areas.

Proposed actions related to cybersecurity education and awareness (p. 8). We concur with many proposals here regarding awareness and outreach efforts to educate members of the public about the importance of cybersecurity and what they can do. As you know, cyberspace's stakeholders—consumers, businesses, governments, and infrastructure owners and operators—need to know how to reduce risks to their property, reputations, and operations. However, many stakeholders are not aware of and also do not adequately utilize the range of tools available to them to do so, such as information sharing, risk management models, technology, training, and globally accepted security standards, guidelines and best practices. Cyberspace's stakeholders should be more aware of risks, aware of how they can secure and protect their things of value, and be responsible for taking action accordingly, just as in the offline world.

We also commend the focus on cybersecurity-oriented education and training. A lack of consistent education and expectation for students and graduates hampers industry's ability to procure, build, deploy, and maintain more secure systems and networks. We urge the Commission to provide any support needed to Member States so that they also prioritize cybersecurity in education. We also strongly endorse the proposal for a synchronized EU-US cybersecurity month starting in 2014, and stand ready to support efforts to make this endeavor successful.

2.2: Drastically reducing cybercrime

We commend section 2.2's proposed actions for the Commission, Member States, Europol, and Eurojust to take to address cyber crimes and criminals, such as strengthening Member States' capabilities to investigate and combat cybercrime, and facilitating a coordinated and collaborative approach at the EU level. As you are aware, there are analogies between the off-line and on-line worlds. These are traditional actors and crimes—the difference is the medium—and traditional laws and government bodies have long been tasked with dealing with them. In

fact, law enforcement and national security are core government functions. Governments can best undertake this responsibility in both the off-line and on-line worlds with the right laws, efforts, and information sharing practices. Again, we applaud the Communication's proposed actions in this area.

2.3: Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)

No comments.

2.4: Developing the industrial and technological resources for cybersecurity

ITI is concerned that many of the proposed actions in this section take static, prescriptive approaches that would result in decreased, not increased security. At the same time, we agree with many recommendations in this section, namely exploring incentives and fostering R&D, as explained in the last portion of our comments on section 2.4

Introduction (p. 12). We commend the fact that European governments and companies are already global leaders in cybersecurity. We are concerned, however, that this introduction equates product security with where or by whom a product is made rather than how a product is made, used, and maintained. Specifically, the first paragraph states "There is a risk that Europe not only becomes excessively dependent on ICT produced elsewhere, but also on security solutions developed outside its borders." We caution that this focus on country of origin could have negative repercussions in two regards.

First, any restrictions on products made "not in Europe" could lead to decreased security of Europe's information systems by restricting European enterprises' qualified suppliers and technologies. The best security products and services can come from anywhere in the world-within the EU, or outside of it. Such restrictions could balkanize the global cyber infrastructure, undermining the interoperability and security of networks globally and resulting in huge negative commercial implications for European and U.S. ICT companies.

Second, an assertion by the EU in this Communication that country of origin equates security would send a very troubling message to the EU's trading partners that such an approach is acceptable or is thought to improve security. In short, if other countries take a cue from an EU focus on country of origin, it could contribute to a "race to the bottom" whereby country after country or region after region invokes a similar rationale to justify excluding foreign companies or technologies, including those from the EU, from their markets. The Commission, in particular DG Trade and DG CNECT, has actively worked over the past few years to discourage the governments of China and India from enacting country-of-origin approaches to product security, namely in China's Multi-Level Protection Scheme (MLPS) and India's Preferential Market Access (PMA) policy, respectively. It is imperative that the EU set an example for others around the world on how address legitimate cybersecurity concerns without disrupting innovation, competition, and global trade flows.

We recommend that other approaches to advancing and promoting European security technologies be considered, such as fostering R&D as described on pp. 13-14 of the Communication.

Promoting a single market for cybersecurity products (p. 12). We suggest that section 2.4 take a more risk-based view of cybersecurity rather than an approach that attempts to guarantee or "ensure" security. We further suggest that this section consider taking a more holistic approach to risk management. A risk framework should focus on properly assessing, managing, and mitigating potential security risks, which comprise threats, vulnerabilities, and consequences and can include people and processes—not just technology. A risk framework also should reflect a role for all participants in the supply chain ecosystem that can contribute to risk management, including purchasers and users. For example, we suggest that security can be most improved if all in the value chain (e.g. equipment manufacturers, software developers, information society service providers, governments, and end-users) make security a priority.

Security standards (pp. 12-13). The global ICT industry is heavily invested in developing security standards to address important challenges in security management. We welcome and encourage governments to participate in standards development activities, particularly in private fora and consortia.

We are pleased that the Commission affirms in its February 2013 "FAQ" memo that the EU does not intend "to define minimum standards or level of security" (p. 5).[4] However, this appears difficult to reconcile with the intention of the draft NIS Directive to adopt a list of EU-endorsed relevant cybersecurity standards (See Preamble 32 and Article 16). ITI strongly cautions all governments not to set compulsory security standards for the commercial market– whether ones vendors must follow as they build their products or services, or standards that would guide consumers when purchasing ICT products and services or conducting business with companies. Such an approach could encourage some firms to invest only in meeting static standards or best practices that are outmoded before they can even be published or cause organizations to divert scarce resources away from areas requiring greater investment towards areas with lower priority. To maintain rather than restrain innovation and to prevent the development of single points of failure, any standards lists should be purely indicative, their use entirely voluntary, and they should always allow organizations to adopt alternative solutions.

We therefore urge the Commission to take a leadership role in promoting the adoption of industry-led, voluntary, globally recognized cybersecurity standards and best practices, make the preservation and promotion of a global market a primary goal in any product assurance requirements, and avoid EU-specific requirements. Defining new, EU- centric standards has many downsides as they may conflict with, global standards currently used, such as the Common Criteria for Information Technology Security Evaluation (CC),[5] or set new trade barriers.

[4] European Commission Memo: Proposed Directive on Network and Information Security—Frequently Asked Questions, February 7, 2013.

[5] The CC is an accepted international standard for computer security certification intended to provide product assurance globally, as well as a multilateral agreement among 26 countries including 13 EU Member States (Austria, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Italy, the Netherlands, Spain, Sweden, and the UK).

In addition, governments can help to promote private-sector adoption of global, voluntary standards and best practices for cybersecurity risk management—by themselves using them and demonstrating their importance. Thus, the Commission and Member States might consider greater action in their own (public sector) use of voluntary, globally accepted standards or generally accepted industry practices. Indeed, government leadership may be necessary to overcome economic disincentives to adoption of standards that yield benefits to the network as a whole rather than primarily to the entity adopting the standard.

Inform authorities on detected vulnerabilities (p. 13). The Commission proposes to "examine how major providers of ICT hardware and software could inform national competent authorities on detected vulnerabilities that could have significant security implications" (third bullet in box).

We caution the Commission not to require, or even urge, ICT vendors to inform authorities about product vulnerabilities before a patch to a particular vulnerability is designed and deployed. No reputable vendor would agree to disclose unpatched vulnerabilities, for multiple reasons: 1) this information could leak, decreasing security of the users it was intended to protect by publicizing exploitable vulnerabilities; 2) it is poor public policy to provide information about unfixed vulnerabilities to one set of customers but not others; and 3) very few customers have the technical ability to use such information, e.g. to develop work-arounds.

Recital 28 of the preamble to the Proposed NIS Directive states: "In the implementation of the notification obligations, competent authorities should pay particular attention to the need to maintain information about product vulnerabilities strictly confidential prior to the release of appropriate security fixes." Although Recital 28 addresses instances when third parties/customers (not vendors) inform competent authorities about vulnerabilities, it still recognizes the importance of keeping vulnerabilities confidential before patches are available.

Security labels/kite marks (p. 13). While labels or kite marks may have a role to play in educating the marketplace about security, government intervention in this area must be carefully calibrated. The correct level of security in any given context will depend on a number of separate considerations. Thus it is imperative that any security labels or kite marks not discourage a correct examination of specific security needs by users. If used, labels or kite marks should be industry-led, global, and voluntary. Governments should remain neutral when it comes to advocating or endorsing particular products, services, or companies via such labels. This is something to be decided by the free market. Any reference to government endorsement in this regard also would send the wrong signals to the EU's trading partners looking to impose market access barriers, under the guise of security, that give preference to one company or nationality of a company/product for "security" justifications. The EU should continue to try to steer its trading partners away from such favoritism and market intervention, and thus should continue to lead by example.

Purchasing power of public administrations (p. 14). Government procurement policy can play a positive role in encouraging the development and adoption of leading-edge technologies. This approach is commonly contemplated by governments but we feel strongly that three core principles are necessary for effective implementation:

1. **Government procurement policies must be technology neutral.** While it is acceptable for procurement policies to specify security objectives, the decisions regarding how to meet those objectives (such as what technologies to use or how or where to build them) must be left up to the vendor that would like to sell to a government entity.
2. **Government procurement policies should avoid mandates on the design and development of products.** This should include how companies run their supply chains.
3. **Government procurement policies should focus on security objectives.** We caution strongly against any procurement approach that would mandate where ICT products are built. Policies should instead focus on the standards, processes, and policies followed during product development.

We think it is reasonable for the Commission to expect development, by the end of 2013, of good practices on how to use the purchasing power of public administration (such as via public procurement) to stimulate the development and deployment of security features in ICT products and services. We would further support an approach in which practices are technologically neutral, avoid mandates regarding how the ICT industry designs and develops its products, including how companies run their supply chains, and avoid mandates regarding where ICT products are built.

Finally, we agree with some key ideas presented in section 2.4.

Fostering R&D investments and innovation (pp. 13-14). We concur with nearly all proposed actions in this portion of section 2.4. We strongly agree that governments have a critical role in promoting and accelerating R&D of key cybersecurity technologies. We have long encouraged the U.S. Government to increase its R&D related to security, to help identify R&D gaps and direct resources to emerging security technologies, and to support industry's R&D, and we have the same recommendations for the Commission. ITI also recommends that the Commission and Member States seek out industry participation in developing strategies and setting priorities related the cybersecurity-related R&D. Further, the Commission and Member States should promote public-private partnerships for cybersecurity R&D, particularly partnerships that include a multi-disciplinary approach involving the ICT hardware, software, and networking sectors.

Finally, the Commission also should determine if cross-border partnerships in R&D would be helpful. It is possible that some of Europe's trading partners—such as the United States—are also interested in pursuing R&D in certain segments of cybersecurity. If so, joining forces to advance R&D will help all of us get to our goals more quickly.

2.5: Establishing a coherent international cyberspace policy for the European Union and promoting core EU values

We concur with this section's emphasis on cross-border cooperation to address the challenges of cyberspace. We particularly appreciate the plan to "place renewed emphasis on dialogue with third countries" (p. 15, second paragraph) and to "support global capacity building in third countries" (p. 16, fourth bullet). For example, capacity-building could include support with law enforcement resources and assistance updating legislative frameworks.

The EU has long been recognized as a global technology leader. European companies have particular expertise in telecommunications network infrastructure, and European technologies led the way in many mobile technologies, such as 3G. We believe that similarly many countries will look to Europe's leadership in cybersecurity policy. Taking a leadership role with regard to one of this decade's pressing technology issues—cybersecurity—is a responsibility that we urge Europe to accept.

But in doing so, it is imperative that the EU signal to governments globally about the approaches that will most effectively improve cybersecurity. Per the DE-ITI-JEITA Joint Statement of 2012, this entails a cooperative approach between government and industry; taking approaches to advance cybersecurity that meet security needs while preserving interoperability, openness, and a global market; and allowing industry to innovate and compete. We fear, however, that some of the Communication's proposed actions, as described in our comments above, diverge from these best practices. We urge the Commission to rethink these proposals. In implementing the Communication, the Commission should:

- Exercise leadership in encouraging the use of bottom-up, industry-led, globally accepted standards, best practices, and assurance programs to promote security and interoperability.
- Make the preservation and promotion of a global market a primary goal in any product assurance requirements, and avoid EU-specific requirements.
- Carefully view any EU policies from a global perspective. Any EU policies that are non-globally compatible, whether implemented through a Directive or a Regulation (or sometimes if merely proposed) will be emulated around the world. Some countries also may use such policies or proposals as a starting point for their own additional domestic regulatory intrusions that will balkanize the global marketplace.
- Proactively seek dialogues with the EU's trading partners about the use and benefits of industry-led, globally recognized standards and best practices that will achieve the requisite levels of security needed to meet national security concerns while preserving interoperability, openness, and economic development.
- Counter other countries' attempts to enact non-globally compatible cybersecurity-related standards, practices and requirements that threaten to balkanize cyberspace and make it less secure.

Conclusion

ITI concurs with the vast majority of the proposed actions in the Communication and our member companies stand ready to work with the EU and Member States to further discuss these ideas so as to improve cybersecurity not only within Europe, but globally.

ITI would like to again thank European policymakers for tackling the important issue of cybersecurity. ITI and its members look forward to working with you over the coming months, and we hope our input will receive due consideration. We are available at any time to elaborate on our comments and our suggestions. Please continue to consider ITI a resource on cybersecurity moving forward.

Please contact Danielle Kriz, Director, Global Cybersecurity Policy
dkriz@itic.org; +1-202-626-5731

Innovation.
Insight.
Influence.

member companies