RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE STUDIES

Policy Paper

Toward an EU Cybersecurity Strategy: The Role of Estonia

Emmet Tuohy

December 2012

Overview:

After a late start, the European Union has recently begun to recognize the extent and severity of the challenges posed by cybersecurity threats. Whereas such concerns were previously restricted to a relatively small circle of technical experts, policymakers are finally becoming aware of the manifold dangers that cyber attacks present to so many areas of society, from commercial banking and intellectual property to energy infrastructure and even military communication networks. And even as the European Commission and agencies such as ENISA have begun to increase their own capabilities in response to these threats, in their efforts to develop a European cybersecurity strategy, they have demonstrated a welcome awareness of the need for intergovernmental coordination and cooperation, especially with member states.

Of course, such a complex set of challenges cannot be solely addressed at the European level, however. In order to further this cooperative process, therefore, all member states have their own roles to play: first, in developing their own capabilities to ensure that there is no "weakest link" in an increasingly interlinked European information space; and second, in developing and implementing policy "best practices" from which other states—and the international community—can learn.

Without the context and direction provided by a clear and considered EU *strategy,* however, the full benefits of individual countries' activity in these ways cannot be obtained. Accordingly, the development of this strategy is a particularly urgent priority—and the **role of Estonia**, with its unique experience and expertise in the field of information technology and cybersecurity, **should be to shape and strengthen this European strategy.**

Why Estonia?

Today, Estonia is widely regarded as a leader in information technology in general, and cybersecurity in particular. This "little country that could"[1]has been the subject of numerous articles extolling it as the homeland of breakthroughs such as Skype, Internet elections, and mobile phone payment systems. And although the rapid transformation of this small Nordic country from an occupied Soviet republic into "E-stonia" surprised many outside observers, this change was not accidental. Estonia's technological leap

[1] Richard Rahn, "Estonia, the Little Country that Could", *Washington Times*, June 20, 2011, available at http://www.washingtontimes.com/news/2011/jun/20/the-little-country-that-could

forward was brought about primarily by the conscious early decision of its political leaders to design and implement a comprehensive programme of education and investment in technology. A brief review of this programme is essential to understanding why Estonia developed its unique capabilities in cyber defence—and how other countries can emulate its example.

Inheriting weak or absent Soviet infrastructure at independence—only half the country's population in 1991 had even a telephone line—the country's young new leaders quickly realized that computer technology could help their country to bridge this gap. Instead of carrying out infrastructure improvements and upgrades using expensive (and often unavailable) existing technology, the government invested heavily in digital solutions: to take one example, the Estonian Border Guard switched to electronic communication as early as 1999, years before its peers elsewhere in Europe. Yet, the centerpiece of Estonia's investment in technology—and arguably the key factor behind its rise to prominence in the sector—was the Tiger's Leap (*Tiigrihüpe*) program of computing in education. First proposed by Ambassador (now President) Toomas Hendrik Ilves in 1996, and developed with Minister of Education and Research Jaak Aaviksoo, the Tiger's Leap was implemented rapidly. By 1997, fully 97% of Estonian schools had Internet access.

The graduates of these schools brought their skills with them when they moved into the workforce, further driving innovation both in the commercial and public sectors, where startup firms and e-government initiatives quickly sprouted. Moreover, the dramatic pace of this innovation was matched by a commitment to sound design principles; individual initiatives were tested and perfected via pilot programmes before being introduced to the general public. Indeed, the testing process for one of the most significant e-government initiatives—electronic voting—that directly led to the establishment of effective cyber defence capabilities in Estonia.

Utilizing the capabilities of the national ID card (a microchip-implanted document linked to a secure database), Estonia held its first legally-binding e-vote in certain municipal elections in 2005 before planning to expand the system to the entire country in time for the March 2007 parliamentary ballot. As they prepared to ensure the integrity of the election, Estonian officials—who had established a Computer Emergency Response Team (CERT) the previous year—identified and prepared responses to several security issues that came up during the testing process; chief among them the risk of external computer attacks on the system itself. While the election was conducted successfully, these new cyber defences would be tested far sooner than anyone expected. Just weeks later, on May 9, Estonia was hit with a cyber attack unprecedented in world history; as journalist Joshua Davis observed, "never before had an entire country been targeted on almost every digital front all at once."[2]

After escaping the 2007 attacks without significant lasting damage, Estonia has continued to be a leader in the field of cyber defence planning and innovation; for example in lending assistance to the Georgian government as it faced even more severe cyber attacks during its August 2008 war with Russia, as well as in creating and hosting the NATO centre of excellence on cybersecurity, which received full accreditation in October of that same year.

[2] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe", *Wired* vol. 15, issue 9 (August 21, 2007), available at http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all

Recommendations: How Estonia Can Help the EU

After a period of inaction, the European Union has finally begun to address and take seriously the need to adopt a cybersecurity policy of its own. It is a welcome step that, in recent months, senior policymakers such as Neelie Kroes and Catherine Ashton have demonstrated a clear understanding of these issues. Now that the EU is ready, in Ashton's words, to "harmonize the readiness of EU countries to deal with security challenges in cyberspace"[3] by drafting a comprehensive cybersecurity strategy, it is time for Estonia to use its experience and expertise to help its European partners in this process.

The most constructive way forward for Estonia in doing so is to **identify existing strengths** within the emerging EU cybersecurity consensus, and then **find ways to build on them**. This is more likely to be helpful—and more successful—than alternative approaches such as an overly negative critique of current flaws within EU strategic thinking on cybersecurity, or an overly positive endorsement that may result in critical gaps in future policy. A review of **four** such strengths, **public-private sector cooperation, inter- and intragovernmental coordination, resilience,** and **avenues for further research** will illustrate the effectiveness of this approach.

1) Public-private sector cooperation

First, EU leaders have begun to recognize the centrality of public-private sector cooperation in any cybersecurity strategy. It is now clear that it is the commercial sector that is most at risk—and most often victimized—by cyber attacks. Although some firms in some sectors remain worryingly exposed to these dangers, by necessity the private sector has in recent years developed considerable expertise in protecting intellectual property and other valuable commercial resources.

Building on this consensus view, Estonia should propose concrete ways of fostering such cooperation at the European level. Certainly, not all elements of the Estonian approach, formed as it is in a small country with a remarkable level of trust among both parties in the business-government partnership, can be transferred directly elsewhere. Yet, even solutions rooted in uniquely Estonian societal conditions—such as universal conscription—can help to increase the extent and effectiveness of public-private sector cooperation elsewhere.

For example, the most prominent form of such cooperation in Estonia is the Cyber Defence League (CDL), an integral part of the country's reserve armed forces. Charged with defending "Estonia's high-tech lifestyle, protecting information infrastructure, and thereby carrying out broad-based national defense objectives,"[4] the CDL is comprised of specialists and volunteers with relevant IT skills who serve on a part-time basis. Since members continue to work in their private-sector positions, both government and business benefit from the increased resources and knowledge. Moreover, just as in other reserve defence forces, CDL volunteers develop greater familiarity and experience working together—a critical asset in any future crisis situation.

---

[3] "Cyber Security: An Open, Free, and Secure Internet", European Union External Action Service press release, October 8, 2012, available at http://eeas.europa.eu/top_stories/2012/081012_cyberspace_en.htm

[4] "The Defence Forces and the Defence League," *Eesti.ee* [Estonia State Portal], available at https://www.eesti.ee/eng/riigikaitse/eesti_kaitsejoud/kaitsevagi

While the specifically military nature of the CDL makes it unsuitable to be applied directly to other member states, particularly those with different experiences regarding conscription, this does not make the example irrelevant. **In light of the difficulty of attracting and retaining top cyber talent to public-sector employment, the EU and member states should consider establishing programmes by which technical experts from the private sector can work in government on a part-time and/or voluntary basis.**

2)Inter- and intragovernmental coordination

Second, there is now widespread agreement in the EU that the shifting, fluid nature of the cyber threat makes coordination *among* governments absolutely essential. As ENISA head Udo Helmbrecht has recently noted, there is a wide gap in capabilities among member states' CERT teams, making coordination extremely difficult. This capability gap stems not only from funding differences, but also administrative and structural inconsistencies. It is difficult for European CERTs to work together effectively when such disparities exist. The following partial listing illustrates the problem:

> In the United Kingdom, the Netherlands, France and Ireland, CERTs are hosted by national cybersecurity centers that have at least some responsibility for the country's national cybersecurity strategy. In Finland, Bulgaria and Romania, CERTs are overseen by national telecommunications regulatory authorities. The Danish GovCERT is hosted by the Danish Ministry of Defence, and NorCERT is a part of Norway's national security agency, while Italy and Cyprus have no official national or governmental CERT in operational mode."[5]

In Estonia, where the CERT is a key part of the Estonian Information System's Authority (ESIA), itself part of the Ministry of Economic Affairs and Communications, the system has worked relatively smoothly because of the clear way in which it delineates authority and responsibility. In order to attain the same benefits at the European level, the current situation—in which, as President Ilves has pointed out[6], responsibility for cybersecurity is divided among four directorates-general—demands reform. Accordingly, **the EU should consolidate responsibility for cybersecurity planning** under one "roof", likely that of ENISA.

3) Resilience

Another welcome shift in EU thinking on cybersecurity has been that of embracing cyber network *resilience* as a strategic priority. In contrast to security, which focuses on preventing or repelling outside threats, resilience can be defined as the ability to manage reductions/interruptions in service provision without significant broader societal disruption.[7] Estonian cybersecurity policy has reflected principles of resilience

---

[5] Jennifer Baker, "EU Cybersecurity Agency Says Variation Between Countries Adds Risk, *CIO,* December 17, 2012, available at http://www.cio.com/article/724162/EU_Cybersecurity_Agency_Says_Variation_Between_Countries_Adds_Risk

[6] Toomas Hendrik Ilves, "E-Governance and Cyber-Security: When Small Means Big, or Why You Can't Bribe a Computer", remarks delivered at the Center for Strategic and International Studies, Washington, D.C., April 12, 2012

[7] Charles Perin III and Emmet Tuohy, "Energy Security Begins at Home: The US Experience and the Role of Efficiency Gains in Promoting Energy Resilience", *Energy Security Forum* 3:6 (November 2012), p. 4

virtually from the start. Perhaps the best example is this rule from the 2007 CERT crisis response guidelines: " If something goes down and it is not really vital, let it *be* down until there is enough free time to bring it back up."[8]

As more and more key governmental and economic functions have expanded into cyberspace, however, they have sometimes moved beyond the reach of highly-trained technical "triage" teams like Estonia's CERT. One such critical area is that of energy infrastructure, as demonstrated by the recent case of 50Hertz. In December, the German electricity supplier of over 18 million customers was hit by a five-day-long cyberattack that brought down the company's communications system—and could have done much greater damage. Its CEO frankly admitted that "[this incident] shows that we have to take cybersecurity seriously," while the chief executive of its parent company acknowledged that "we weren't aware of the [cyber] risk five or ten years ago."[9]

To prevent similar attacks, and to ensure the continued resilience of cyber networks and all that depends on them, **governments should maintain close attention to the cybersecurity policy implications of changes to critical infrastructure.** In the above example, the EU had mandated as part of the Third Energy Package that 80% of European electricity providers be equipped with electronic "smart meters" by 2020. While this goal is laudable, it remains worrying that it was adopted without any consideration of the security risks that result in moving such a large share of critical infrastructure into the digital domain.

4) Avenues for Further Research

Lastly, perhaps the most salutary trend within the EU has been the growing support for research efforts. There is a widespread sense that the European academic and policy communities ought be involved in the global discussion about cybersecurity, whether in promoting training for young experts at the school level, or in funding R&D efforts at the technical level.

These are welcome initiatives; but in the end, it is better to *shape* the global discussion than merely to be involved in it. With its experience of multilateral intiatives and its expertise in creating broader legal norms, the EU is particularly well-suited to taking a global lead in resolving conceptual areas of cybersecurity strategy. Yet, to this point, the EU has refrained from contributing to the international debate on one key aspect: *offensive* capability.

As recent controversies over the tailored Stuxnet virus in Iran have demonstrated, there is a crying need for the development of clear doctrine on when and how offensive capability should be developed, and more importantly, when (and how) it should be used. Certainly, the lines are blurry in cyberspace: often, cyber operations that take place outside one's network are actually defensive in nature. Yet, with other complex areas of international law such as genocide tribunals or freedom of expression, the EU has already taken a clear stance in helping to shape viable global norms.

Ultimately, in the sphere of cybersecurity, it is Estonia that has—and must continue to—define and promote these kinds of standards. Even prominent critics of of

---

8 Merike Kaeo, "Cyber Attacks on Estonia: Short Synopsis", n.d., Double Shot Security, available at http://www.doubleshotsecurity.com/pdf/NANOG-eesti.pdf

9 "European Power Grid Rocked by Cyber-Attack", EurActiv, December 10, 2012, available at http://www.euractiv.com/energy/european-renewable-power-grid-ro-news-516541

cybersecurity investment such as University of Glasgow professor Brandon Valeriano acknowledge that Estonia has "become a great leader in promoting cyberspace rules and norms that keep states...in line."[10]

After its experience on the receiving end of the world's first major cyberattack in 2007, Estonia's diplomatic response has been quite unique. Instead of seeking revenge, it has sought to build a broader international consensus, firmly based on existing principles of international law. In this respect, **the best thing that Estonia can do for European cybersecurity is to convince its EU partners to join it in its effort to construct viable international norms for cyber defence, including offensive capabilities,** so as to ensure that such an attack can never occur again.

[10] Brandon Valeriano and Ryan Maness, "The Fog of Cyberwar", *Foreign Affairs,* November 21, 2012, available at http://www.foreignaffairs.com/articles/138443/brandon-valeriano-and-ryan-maness/the-fog-of-cyberwar?page=2&cid=nlc-this_week_on_foreignaffairs_co-120612-the_fog_of_cyberwar_3-120612