IMAGE – SHUTTERSTOCK

2007 cyber attacks on Estonia

NATIONS INVOLVED: Estonia, Russian Federation

TIME PERIOD: April 2007 – May 2007

THEMATIC AREA: Cyber Operations

EXECUTIVE SUMMARY

In April and May 2007, Estonia became the target of a coordinated cyber attack. Over a three-week period, government and parliamentary portals, ministries, news outlets, internet service providers, major banks, and small businesses were all targeted, predominantly by a Distributed Denial of Service (DDoS). The cyber attack coincided with the Estonian government's decision to relocate the 'Bronze Soldier Memorial' in Tallinn, which led to significant civil disturbance in both Estonia and Russia.

The vast majority of malicious network traffic was of Russian-language origin and had indications of political motivation. The Russian government denied any involvement; however, the cyber attacks were accompanied by hostile political rhetoric by Russian officials, unfriendly economic measures, and refusal to cooperate with the Estonian investigation in the aftermath of the attacks, all of which likely encouraged the perpetrators.

The attacks caused some disruption and economic cost to Estonia. Perhaps more importantly, though, they exposed Estonia's vulnerabilities, and demonstrated the *potential* of cyber attacks to cause far more lasting damage if intended. However, the incident also demonstrated Estonia's capabilities and resilience in countering the cyber attacks. Ultimately, the shock caused by the cyber attack led to a significant strengthening of cyber defence capabilities, institutions and legislation in Estonia, the European Union, and NATO.

KEY POINTS

■ **Ambiguity** was a key feature of this cyber attack. As the attacks were apparently carried out independently by individuals using their own resources, any state sponsor responsible for orchestrating the attack was able to disguise and deny themselves as the source. This underscores the requirement for governments to achieve political consensus on attribution in a timely manner based on the available evidence and be able to communicate this in a clear and understandable way to the general public.

■ In addition to the physical effect on infrastructure, cyber attacks have a significant **psychological dimension**. In this case, attackers could have inflicted significantly more damage within the cyber domain if desired, but it was highly likely that a key objective was to test and demonstrate cyber capabilities, as well as to sow confusion and uncertainty.

■ In this case, as well as in similar cyber attacks on Lithuania (June 2008), Georgia (July/August 2008), and Kyrgyzstan (January 2009), cyber activity was **integrated and synchronised** with a **wide spectrum of other measures**, such as economic or diplomatic pressure, with the result of increasing strategic effects.

SUMMARY

In the spring of 2007, three weeks of globally Distributed Denial of Service (DDoS) cyber attacks, apparently the spontaneous acts of pro-Russian individuals and groups, targeted Estonian governmental, political, financial, and other websites and e-services. This event is widely regarded as the first major act of cyber warfare in the world. Modified attack tools, shared in forums by Russian (or Russian-language) hackers and, later, 'rented' botnets nearly blocked Estonia's access to the internet completely. Two waves of attacks occurred – the second significantly more sophisticated than the first.

The attacks were an apparent response to the Estonian government's intention to relocate a Soviet-era war memorial (the Bronze Soldier and burial place of Tallinn). Protests by activists from Estonia's Russian community faded, to be followed by what is assessed to be (particularly with the second wave) a planned and professionally orchestrated cyber attack. As many as 1-2 million pre-infected 'bots' in 175 jurisdictions were organised to launch a coordinated attack on Estonian targets by flooding websites with data. 174 jurisdictions supported Estonia in resolving the attacks: only the Russian Federation did not. Russia denied any involvement and pointed to a relatively minor hack it had suffered as proof that it too was a target.

The initial low-tech attacks began on 26 April, the day the excavation works began, followed by a much more sophisticated and well-coordinated attack beginning on 4 May and peaking on 9 May (Victory Day, a national holiday in the Russian Federation which commemorates victory over Nazi Germany in the 'Great Patriotic War'). The attacks were dynamic, changing in response to counter-measures and ceasing at a precise time and also synchronised to other actions by Russia that were hostile to Estonia, such as the severing of commercially important rail links, with no notice, for alleged 'repairs'.

Estonia faced lost productivity, opportunity cost, remediation, and the acquisition of alternative web hosting at emergency rates estimated to be in the billions of Euro. However, the stability of some Estonian inventions (e.g. Skype) and the means by which the state drew on internal and mutual aid from other countries means that its reputation, resilience, and capability were ultimately strengthened by these attacks. The attack could have resulted in a weakening of Estonian citizens' trust in the government's ability to defend the country against unconventional attacks, but the quick response of the government, together with support from NATO and many nations in ensuring recovery, prevented widespread public distrust. It is assessed that the cyber attacks had no significant effect on any internal divisions between Estonian citizens of differing linguistic and ethnic heritage.

CONTEXT

Distributed denial of service (DDoS) attacks are one of the most common forms of cyber attack. For a DDoS attack to be successful, the attacker will spread malicious software to vulnerable computers, e.g. through infected emails and attachments, and so create a network of infected machines (called a botnet). The attacker can then command the botnet to bombard a certain website or online service with traffic, until the site crashes under the sheer load of requests.[1] DDoS attacks, by their nature, do not usually cause extensive or even irrecoverable damage, but can cause considerable disruption. It is difficult to prevent DDoS attacks (e.g. by creating a better firewall), since it is difficult to distinguish between legitimate and illegitimate traffic.

Highly effective cyber, reconnaissance and target selection, and development and coordination of criminal operators to undertake the attack – presumably for money – make it easy for state actors to deny any involvement, reinforced by the technical sophistication to make attribution of modified attack tools challenging. The 2007 attack on Estonia was developed using fairly crude Internet Control Message Protocol (ICMP)[2] floods, email bombing encouraged through internet forums, and more challenging DDoS attacks using networks of hijacked botnets, culminating in a devastating effect.

Bronze Soldier Memorial in its new location. IMAGE – SHUTTERSTOCK

[1] Christina Mercer, "What is a DDoS Attack? What Happens During a DDoS Attack?" Techworld, 17 May 2017, *https://www.techworld.com/security/how-does-ddos-attack-work-3659197/*

[2] For details on ICMP and why it matters: *http://searchnetworking.techtarget.com/definition/ICMP*

Timeline of Key Events

10 January 2007
Government's plan to relocate the "Bronze Soldier" announced

26-27 April 2007
Excavation works begin around the Bronze Soldier Memorial in Tallinn. Due to violent street protests, authorities decide to speed up the removal of the statue.

27 April – 19 May 2007
Cyber attacks on Estonia:

27 April 2007
First wave of un-coordinated attacks on high-profile websites begins, targeting the President, Parliament, police, political parties, and major media outlets.

28 April 2007
Co-ordinated fight-back effort of the Ministry of Defence in cooperation with CERT-EE begins, supported by other CERTs around Europe.

4 May 2007
Second, more advanced wave of cyber attacks, this time also targeting banks (especially Hansabank and SEB Eesti Uhisbank).

9 May 2007
'Victory Day' celebrated in Russian Federation. Attacks peak.

19 May 2007
Cyber attacks abruptly and simultaneously cease.

January 2008
Estonian government indicts one of the responsible hackers.

January 2008
NATO approves its first policy on cyber defence.[3]

May 2008
The Estonian Ministry of Defence implements a National Cyber Security Strategy.[4]

[3] Warwick Ashford, "Cyber Threats are Among Top Dangers, Says Nato," *Computer Weekly*, 11 October 2017, *http://www.computerweekly.com/news/450428006/Cyber-threats-are-among-top-dangers-says-Nato*

[4] Estonian Ministry of Defence, *Cyber Security Strategy*, 2008, *http://www.sicurezzacibernetica.it/db/[Estonia]%20%20National%20Cyber%20Security%20Strategy%20-%20old%20-%202008%20-%20EN.pdf*

Estonian Government Narratives

- **The Bronze Soldier memorial symbolises occupation and deportation for many Estonians. For others, it symbolises grief and the memory of the dead. Moving the statue and the remains from the city centre to a cemetary is more suitable, and will help societal unity.**
- **These cyber attacks are a blatant attack not only on Estonia's sovereignty, but also on the entire European Union.**
- **The Russian government is at least indirectly responsible for these cyber attacks.**
- **As Estonia is one of the most digitally advanced states in the world, the cyber attack was countered very effectively.**
- **There is an urgent need to adapt and expand national and international law to address new threats such as cyber attacks.**

Urmas Paet, Minister of Foreign Affairs (2005-2014)

1 May 2007: "The attack is virtual, psychological and real – all at the same time. [...] IP addresses have helped to identify that the cyber terrorists' attacks against the Internet pages of Estonian government agencies and the Office of the President have originated from specific computers and persons in Russian government agencies, including the administration of the President of the Russian Federation."[5,6]

Andrus Ansip, Prime Minister (2005-2014)

2 May 2007: "A physical attack against the Ambassador of Estonia to Moscow [...], together with the continuing cyber attacks from the servers of Russian state authorities, together with tearing the Estonian flag off our embassy and together with statements made by the delegates of the Russian Duma, calling for the change of government in Estonia, indicates that our sovereign state is under a heavy attack. All these events evidence that these are not our internal matters we are dealing with but it is a well-coordinated and flagrant intervention with the internal affairs of Estonia."[7]

Toomas Hendrik Ilves, President (2006-2016)

18 June 2007: "[The cyber attacks] were definitely more than common criminal activity. Someone paid a whole lot of money to afford the service of internet criminals. When you look at the development of the attacks, it is striking that they cease at exactly midnight. I asked CERT what this meant. And I was told: Well, that's just how long they paid for attacks that day. That means it was organised [...]. We do not know who was behind [the cyber attacks]. But we do know that since three years, every internet service provider in Russia is required by law to connect its cables with the secret service FSB. The FSB controls the internet there."[8]

IMAGES – SHUTTERSTOCK and WIKIMEDIA / Estonian Foreign Ministry

[5] "Declaration of the Minister of Foreign Affairs of the Republic of Estonia," Estonian Government Website, 1 May 2007, *https://www.valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia*

[6] However, these Russian computers were most likely also hijacked, like many other computers from Egypt or South America – when their users opened an infected attachment or visited a site that automatically installed malware: Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, 21 August 2007, *https://www.wired.com/2007/08/ff-estonia/*

[7] Andrus Ansip, "Prime Minister Andrus Ansip's Speech in Riigikogu," Estonian Government Website, 2 May 2007, *https://www.valitsus.ee/en/news/prime-minister-andrus-ansips-speech-riigikogu.*

[8] Toomas Ilves (translated from German), "Interview: 'Ist ein Internetangriff der Ernstfall?'" *Frankfurter Allgemeine Zeitung*, 18 June 2007, *http://www.faz.net/aktuell/politik/ausland/estland-im-visier-ist-ein-internetangriff-der-ernstfall-1436040.html*

Ene Ergma, President of the Estonian Parliament (2003-2006, 2007-2014)

21 August 2007: “Estonia is a NATO country. Attacking us is one way of checking NATO’s defenses. They could examine the alliance’s readiness under the cover of the statue protest.”[9]

NATO Narratives

- **Technical assistance and political solidarity for Estonia.**
- **Cyber attack treated as a serious security issue.**

James Appathurai, Spokesperson

23 May 2007: “I think what is clear is that these kinds of attacks are very hard to trace in any sort of definitive way and that is one of the great challenges that one faces in terms of cyber defence. So I cannot speak to the origins of these, but certainly the Estonians have spoken at some length about where they think these attacks are coming from.”[10]

Jaap de Hoop Scheffer, Secretary General (2004-2009)

25 May 2007: “These cyber attacks have a security dimension without any doubt and that is the reason that NATO expertise was sent to Estonia to see what can and should be done. […] Does this have a security implication? Yes, it does have a security implication. Is it relevant for NATO? Yes, it is relevant for NATO. It is a subject which I am afraid will stay on the political agenda in the times to come.”[11]

IMAGES – SHUTTERSTOCK and WIKIMEDIA / Estonian Foreign Ministry. Ene Ergma – IMAGE: WIKIMEDIA / Riigikogu Kantselei, 2011

[9] Ene Ergman quoted in: Joshua Davis, ”Hackers Take Down the Most Wired Country in Europe,” *Wired*, 21 August 2007, *https://www.wired.com/2007/08/ff-estonia/*

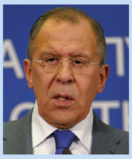
[10] James Appathurai, ”Press Briefing,” *NATO*, 23 May 2007, *https://www.nato.int/cps/en/natohq/opinions_8313.htm?selectedLocale=en*

[11] “NATO Sees Recent Cyber Attacks on Estonia as Security Issue,” *DW*, 26 May 2007, *http://www.dw.com/en/nato-sees-recent-cyber-attacks-on-estonia-as-security-issue/a-2558579*

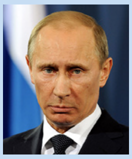
Russian Government Narratives

- **The Estonian government's decision to move the Bronze Soldier memorial is disrespectful and sacrilegious; it will have serious consequences on bilateral relations.**
- **Claims that the Russian government orchestrated the cyber attacks are a lie.**
- **"Patriotic" Russian groups and individuals were involved in the cyber attacks independently from the Russian state.**

Sergei Ivanov, First Deputy Prime Minister (2007-2008)
3 April 2007: Ivanov called on Russians to boycott Estonian goods and services in response to Estonia's plans: "Don't buy Estonian products [...], don't go to Estonia for vacations, go to Kaliningrad."[12]



Sergey Viktorovich Lavrov, Foreign Minister (since 2004)
26 April 2007: "I believe that all this [the removal of the memorial and the ensuing clashes] is disgusting. Although I have not seen any footage yet, I have heard what is happening there. There can be no justification for this blasphemy. It will have serious consequences for our relations with Estonia."[13]



Putin, President (2000-2008, 2012-present)
9 May 2007: During a speech to Russian troops to celebrate Russia's victory over Nazi Germany: "Those who attempt today to [...] defile the monuments to war heroes are insulting their own people, sowing discord and new distrust between states and people."[14]

Dmitry Peskov, First Deputy Press Secretary of the Russian President (2004-2008)
17 May 2007: "[There is] no way the [Russian] state [could] be involved in cyber terrorism [...]. When you look at the IP addresses showing where the attacks are coming from, then there's a wide selection of states from around the world. But it does not mean that foreign governments are behind these attacks. Moreover, as you probably know, IP addresses can be fake."[15]

IMAGES – SHUTTERSTOCK and WIKIMEDIA / Estonian Foreign Ministry

[12] Sergei Ivanov quoted in: "Here We Go Again," *The Baltic Times*, 4 April 2007, *https://www.baltictimes.com/news/articles/17635/*

[13] "Transcript of Remarks and Replies to Media Questions by Russian Minister of Foreign Affairs Sergey Lavrov Following Ministerial Meeting of Russia-NATO Council, Oslo, April 27, 2007," *The Ministry of Foreign Affairs of the Russian Federation*, *http://www.mid.ru/en/press_service/minister_speeches/-/asset_publisher/7OvQR5KJWVmR/content/id/375128*

[14] Vladimir Putin (translated), "Speech at the Military Parade Celebrating the 62nd Anniversary of Victory in the Great Patriotic War," *Kremlin.ru*, 9 May 2007, *http://en.kremlin.ru/events/president/transcripts/24238*

[15] Dmitry Peskov quoted in: "The Cyber Raiders Hitting Estonia," *BBC News*, 17 May 2007, *http://news.bbc.co.uk/2/hi/europe/6665195.stm.*

MEASURES

Strategic Logic

This DDoS attack, although disruptive, was both a predictable risk which was relatively easy to counter immediately, but only with external support. The lack of easy and open attribution to a state actor enabled the attackers' ability to deny involvement, but the concurrent economic disruption and the peak of the cyber attack coinciding with the *scheduled* move of the Tallinn monument indicates that it was very likely to be a coordinated act of hostility. The attacks appeared to be spontaneous and self-organised – "patriotic" non-state actors claimed unproven involvement and there was at least one Estonian-based Russian hacker. Additionally, low levels of cyber literacy in the mass media in reporting these events led to multiple narratives about the actors responsible.

It is assessed that the core strategic logic was to implement a range of measures intended as a response to the Estonian government's relocation of a memorial and to test and demonstrate the capabilities to impact negatively on Estonian national security interests. This situation was an ideal opportunity to functionally test cyber weapons in an area where Russia is active (see below for examples from Georgia, Lithuania, etc.). Co-ordination with other strategically ambiguous measures (including severing railways between Tallinn and St. Petersburg, lengthening of border checks, and cancellation of orders from Russian businesses) suggests that a full spectrum of state-directed forces was mobilised. In this case, cyber attacks were integrated with expressions of economic pressure. It is possible that other cyber activities occurred under the cover of the distraction generated by this attack.

Some analysts suggest that Russia sought to demonstrate to Estonian citizens that their own government (and NATO) were unwilling and unable to protect them and pursue the adversary – thereby contributing to Russian strategic objectives of weakening trust and confidence in national governments, especially in the Baltic region, and international collective security structures.[16] The capability to 'turn off' access of a sovereign nation to the internet is certainly a useful one from the perspective of the attacker. The public was confused by official Russian statements denying Russian involvement, and unlikely groups and individuals claiming responsibility for the attack.[17] Assessments point to cyber operations against Estonia – the most concerted and effective to date – as an exercise of the full spectrum of capacity and capability held by the Russian Federation, and probably operationalised through trusted, yet deniable, assets such as criminal gangs, patriotic groups and others. It is reasonable to assume that there was a strong focus on how Estonia (and its partners) sought to manage a response to the attack.

Diplomatic. Public statements by President Putin and other officials protested plans to relocate a Soviet-era war memorial. This stance reinforced support from certain critical domestic bases (e.g. nationalists) and activists of Russian descent. Similar cyber attacks together with strong diplomatic statements of disapproval

[16] Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," *Cooperative Cyber Defence Centre of Excellence*, 2008, *https://ccdcoe.org/multimedia/analysis-2007-cyber-attacks-against-estonia-information-warfare-perspective.html*

[17] BBC News, "Estonia Hit by 'Moscow Cyber War'," 17 May 2007, *http://news.bbc.co.uk/1/hi/world/europe/6665145.stm*

The Riots in April 2007.
IMAGE – Maksim Shmeljov / SHUTTERSTOCK

Police officers near Bronze Soldier.
IMAGE – Maksim Shmeljov / SHUTTERSTOCK

are known to have been used by Russia in Lithuania in 2008[18] (after a law was passed outlawing communist symbols), Georgia in 2008[19] (prior to invasion by Russia, defacing websites, restricting internet traffic, and using criminal gangs to lead the operation), and Kyrgyzstan in 2009[20] (as the US sought to retain access to a strategically important airbase). It seems unlikely that Putin and other Russian officials would issue warnings without also being willing to instruct military and other institutions to prepare to intervene should the target Estonian government not halt their plans – especially if this event was only the cover for an attack that was to be mounted either way.

Information. By targeting media and many other websites, the cyber attack prevented the citizens of Estonia from obtaining information in the way they were accustomed – whether that was in the form of news, updates from the government or political parties, or their bank balance. By interrupting, or making less reliable and instant the access to information and the flow of money, the attack measures targeted the smooth and 'always on' nature of the digitally-dependent state of Estonia. Citizens and others are dependent on the guaranteed access of information which is now almost treated as any other utility. Blocking this access had profound economic and potentially social consequences, and in the case of an attack of longer duration would have been of strategic consequence to Estonia and the hitherto solid perception of it as a safe and stable place to do business. Apparently, there were no attacks on conventional media systems such as television services, so a digital blockade of information was not total by any means, although those platforms that were targeted (such as the daily newspaper *Postimees*) were sometimes entirely inaccessible.

Military. There is no indication in the open literature that any military assets were used in these attacks (although the coordination indicates that this would have been necessary). There were no accompanying military exercises, movement of forces or provocative actions.

[18] After the Lithuanian Parliament passed a law banning Soviet-era symbols, websites were attacked, others defaced, and some DDoS activity occured. In the months leading up to the cyber attacks, Russia refused to compensate Lithuanians for their detention and suffering in gulags, and also interfered in energy provision. At the same time, Lithuania had "blocked talks on an EU-Russia partnership." See: William C. Ashmore, "Impact of Alleged Russian Cyber Attacks," *Baltic Security & Defence Review* Volume 11 (2009): 4-40.

[19] On 19 July and 8 August 2008, DDoS attacks targeted Georgian websites, first restricted to news and government sites and then "financial institutions, businesses, educational institutions, Western media and a Georgian hacker's website." Complementing DDoS operations overwhelming web-servers, SQL injections attempting to maliciously interfere with databases and email flooding occurred, with "patriotic hackers" lending a hand. These events occurred in the months leading up to the Russian Federation's invasion of South Ossetia, with the peak attacks coinciding with the invasion. Attackers were smart, targeting "websites of renting diesel-powered electric generators in order to support the conventional strike against [and denial of] Georgian electrical infrastructure." See: Andrzej Kozlowski, "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan," *European Scientific Journal* Vol. 3 (February 2014): 239-41.

[20] In a suspected attempt to influence the Kyrgyz government to close down a US air base (Manas Transit Center), DDoS traffic was directed at Kyrgyzstan's government, banks, and media websites on 18 January 2009. As a result, almost 80 per cent of internet traffic in Kyrgyzstan was offline. However, as only a small percentage of the population has access to the internet, the Kyrgyz public was largely unaffected. The DDoS traffic was investigated and traced back to servers located in Russia, which led to much speculation that the Russian Business Network (RBN) of hackers was paid by the Russian government to undertake attacks. See: Andrzej Kozlowski, "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan," *European Scientific Journal* Vol. 3 (February 2014): 241.

Economic and Financial. Targeting banks and other institutions indicated that attackers were aware of both the vulnerability of e-services to DDoS disruption, and that these would generate instant disruption and therefore concern to the government, business, and retail customers (ordinary citizens). It is estimated that Estonia "is 97 percent dependent on internet banking."[21] This attack rendered access unreliable at home and unavailable overseas. Hansabank and SEB Eesti Uhisbank were particularly affected by the attacks. The web-interfaces for internet-based services of the two biggest banks in Estonia were offline for about 45-90 minutes, and foreign money transfers were temporarily unavailable.[22] Citizens were denied access to financial services and Estonia was isolated from the world in terms of flows of finance.

Instilling a 'choke hold' on finance was a key element of this attack. The ability to arbitrarily, at will, prevent a government, businesses, and individual citizens from accessing or transferring money is a significant instrument of national power. Finance, as a critical centre of gravity to an economy, and e-services are fundamental to the operation and reputation of a modern state such as Estonia. This includes critical functions such as tax collection and the perception of the state as a safe place to do business and invest.

The concomitant increase of friction at borders, severing of rail links due to unscheduled "repairs," and cancellation of orders reinforced that consequences would be imposed on small and medium-sized businesses as well as on citizens in general; by extension, the entire political-economy was vulnerable.

Intelligence. It is reasonable to assume that intelligence gathering on vulnerabilities and specific target identification occurred, as the attacks were disciplined in nature, and effects were restricted within the borders of the state without causing existential or irrecoverable damage. The initiation of attacks at specific times (for example midnight in Moscow), the reactive management of the attacks, and the precise control over their ending (when the rented botnet time ran out) indicated that intelligence was being collected and analysed during the progress of the attack. Also, given the likely involvement of organised crime networks in the attack, the identification and clearance of these individuals, payment to them and monitoring of their activities would also have required reliable intelligence activity. There is no public reporting on reconnaissance and organisation ahead of the attacks.

Legal. Ambiguity and difficulty of attribution was one of the key characteristics of this cyber attack. Although it is undoubtedly illegal under international and domestic laws, the aftermath of such a cyber attack is almost impossible to prosecute given the difficulty of identifying individuals and structures within Russia or under its control outside its borders. Even if such information were gathered, it would likely be unusable in prosecutorial efforts: the identification would reveal intelligence collection capability; moreover, the evidence gathered would likely be inadmissible because of the way it was obtained.

Although an Estonian student of Russian origin, Dmitri Galushkevich, was arrested, charged, and convicted with one minor element of the attack (targeting a political party's website),[23] its scale indicated that many people were likely involved in its planning, execution, monitoring, and funding. Some individuals within the Russian political establishment have claimed to have been involved – e.g. an assistant to a Duma member, as have individuals in contested locations such as Transnistria (e.g. Konstantin Goloskokov, a "commissar" of the apparently Russian state-supported youth organisation 'Nashi').[24] Legal observers note that if individuals coordinating or performing

[21] Tom Espiner, "Estonia's Cyberattacks: Lessons Learned, a Year on," *ZDNet*, 1 May 2008, *http://www.zdnet.com/article/estonias-cyberattacks-lessons-learned-a-year-on/*

[22] Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," *International Affairs Review*, 4 April 2009, *http://www.iar-gwu.org/node/65*

[23] Ibid.

[24] Juhan Tere, "The Financial Times: Kremlin-backed Group Behind Estonia Cyber Blitz," *The Baltic Course*, 1 March 2009, *http://www.baltic-course.com/eng/baltic_states_cis/?doc=10962*

the attack operated from jurisdictions such as Transnistria, were assistants to members of parliament or worked in criminal enterprises, then cooperation with investigation and extradition would be highly unlikely.

A Finnish cyber expert, Mikko Hyppoenen, noted that it would be difficult to prove the Russian state's responsibility, and that the Kremlin would be able to inflict a lot more cyber damage if it chose to do so,[25] such as an attack on national power grids, energy, and industrial processes. Supervisory Control and Data Acquisition (SCADA) and other wider critical national infrastructure operations do not appear to have been targeted (perhaps because it would be difficult to mask this as the work of unsophisticated patriotic spontaneous actors). Some analysts conclude that an attack on SCADA "could evoke article V and the response [from NATO could have been] more serious."[26] Falling short of the threshold for invoking Article V was likely a strategic imperative for the Russian Federation: "Because of economic interdependence and the threat of nuclear escalation, Russia cannot risk attacks on NATO member states, perhaps making unattributable cyber strikes an attractive alternative."[27]

[25] Mikko Hyppoenen quoted in: Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, 17 May 2007, *https://www.theguardian.com/world/2007/may/17/topstories3.russia*

[26] Andrzej Kozlowski, "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan," *European Scientific Journal* Vol. 3 (February 2014): 240, *https://eujournal.org/index.php/esj/article/view/2941/2770*

[27] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (Summer 2011): 53, *http://scholarcommons.usf.edu/jss/vol4/iss2/4*

NATIONAL SECURITY INTERESTS

Every state is dependent on access to the internet for the efficient administration of the country, the flow of finance, access to and exchange of information, and the provision of services to citizens and commerce. Access to the internet in Western liberal democracies is provided through private companies and infrastructure. The internet is without doubt a key element of a state's critical national infrastructure, and interruption in the availability of any service that relies on it will have swift, profound and sometimes irreversible consequences (e.g. irrecoverable positions; opportunity costs). Estonia – sometimes dubbed 'E-stonia' – was, and is, one of the world's most digitally connected societies.[28] In 2007, internet-based services for regular banking, provision of government, and other services (such as voting) as well as economic growth were significantly driven by the high-tech sector (e.g. Skype was invented there). Some analysts have suggested the DDoS attacks might have been used to distract from the collecting of other information, conducting attacks, or cyber espionage.[29] However, no publicly available information confirms this.

Critical Functions

Political. A key national security interest for Estonia is to both be and project a sense of being a politically stable, well-governed, and secure state, despite the presence and intent of its eastern neighbour and former occupier. Given its history of occupation and the forced expulsion of individuals to Russian labour camps, Estonia is exceptionally keen to have a political ecosystem which ensures transparency and minimises the perceived distance between citizens and government. As a relatively young nation, playing a leading role in the EU, and the avowed commitment to the Baltic nations from the EU and NATO, when Estonia called for help it was made available. Estonia was the original "wired society," with "all government services available online" and as many as 5.5 per cent of voters having voted electronically in 2007[30] – in a system described by Mihkel Tammet, the IT director of the Estonian Defence Ministry as "paperless government."

Military. The first responsibility of the military forces of a state is to ensure that it is defended from adversaries who would seek to do it harm through the exercise of force. While cyber defence was not mentioned in Estonia's National Defence Strategy of 2005 – it was only included in the 2011 National Defence Strategy – the growing importance of cyberspace was recognised in Estonia's National Security Concept of 2004: "The constantly increasing rate at which electronic information systems are adopted in Estonia, and their connection with and dependence upon worldwide information systems, increases the threat of computer crime as well as the vulnerability of information systems, including spheres of primary importance to national security. [...] To prevent computer crime and threats to internal security, which could arise from the vulnerability of IT

[28] In *The Economist Intelligence Unit's* 2007 e-readiness rankings, Estonia ranked number one in Central and Eastern Europe in the categories "Business Environment," "Government Policy and Vision," and "Consumer and Business Adoption." Estonia also embraced e-democracy, being the first country in the world to offer internet voting in local elections in 2005, as well as in national parliamentary elections in 2007.

[29] Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," *NATO Cooperative Cyber Defence Centre of Excellence,* 2008, *https://ccdcoe.org/multimedia/analysis-2007-cyber-attacks-against-estonia-information-warfare-perspective.html*

[30] Andrzej Kozlowski, "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan," *European Scientific Journal* Vol. 3 (February 2014): 238, *https://eujournal.org/index.php/esj/article/view/2941/2770*

systems, as well as to ensure the security of national data bases and registries, necessary organisational, information technology, and physical security measures are being implemented."[31]

Economic. It is the strategic requirement of any state to ensure that business can occur within and across its borders. Fundamentally, this must be reliable and enable the movement of funds within borders and outside of them. Estonia has built up a reputation as a business-friendly state where start-ups are massively incentivised, and where tax collection is transparent and efficient. This reputation is a valuable resource for a country looking to develop a sustainable economy and to be open to entrepreneurs worldwide.

Social. Considering the significant Russian-speaking community in the Estonian population (about a quarter of the population),[32] and the history of the Russian Federation in manipulating these populations to strategic benefit by promoting instability, the Estonian government is very keen to ensure that opportunities to deepen and broaden any cleavages between Estonians with Russian heritage and those without are effectively countered.

Information. Liberal democratic systems and populations such as Estonia depend upon the free flow of information. As noted earlier, the internet and services (web-page, apps, etc.) that depend on it for intra- and inter-national communications is a vital part of the critical national infrastructure. In 2007, "60 percent of the country's population used the Internet on a daily basis."[33] Newspaper and other media use the internet as their key or at least a major platform for reaching readers and generating income through subscriptions and advertising. The media also has a critical role in the scrutiny and holding of politicians and others to account – as well as the more prosaic, but vital task of being the trusted means by which individual citizens and industry sectors acquire news. Without access, citizens are less informed about events. They may then seek to use social media and potentially other less reliable platforms and sources to gather information. This may make them vulnerable to misinformation (deliberate or accidentally generated).

Infrastructure. As noted earlier, information which flows across networks and the networks which enable this in a timely, reliable, secure manner essentially constitute a utility which sustains many elements of a state's essential services. Estonia built a significant amount of its business-friendly marketing and investment around it being a state with exemplary infrastructure provision. For instance, it is estimated that Estonia "is 97 percent dependent on internet banking."[34] It is therefore a matter of national security that this be demonstrably reliable and secure.

Vulnerabilities

High reliance on technology, limited investment in counter-measures: Estonia's highly-developed information infrastructure (probably in common with many states at that time in the West) was susceptible to interruption from DDoS – a form of attack which is far from being the most creative and destructive of cyber threats. With information infrastructure in private hands, some researchers concluded that the protection of "online borders" should have been more robust: "A DDoS attack may be prevented simply by installing better firewalls around a web site (for example), but no nation currently has the power to tell its ISPs (internet service providers), telecommunications companies and other online businesses that they should do this, which leaves

[31] National Security Concept of the Republic of Estonia (2004), *https://www.files.ethz.ch/isn/156841/Estonia-2004.pdf*

[32] "Disquiet in Baltics over Sympathies of Russian Speakers," *Reuters*, 24 March 2014, *https://www.reuters.com/article/us-ukraine-crisis-russia-insight/disquiet-in-baltics-over-sympathies-of-russian-speakers-idUSBREA2K07S20140324*

[33] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (Summer 2011): 51, *http://scholarcommons.usf.edu/jss/vol4/iss2/4*

[34] Tom Espiner, "Estonia's Cyberattacks: Lessons Learned, a Year on," *ZDNet*, 1 May 2008, *http://www.zdnet.com/article/estonias-cyberattacks-lessons-learned-a-year-on/*

the country wide open to cyber strikes."[35] This culminated in a situation where, albeit briefly, "Estonia has built their future on having a high-tech government and economy, and they've basically been brought to their knees because of these attacks."[36]

DDoS vulnerability: Distributed Denial of Service attacks exploit the vulnerability of unprotected web-sites and web-enabled resources to succumb to the direction of massive amounts of internet traffic. Automated and reactive measures could have been put in place to ensure that this vulnerability was prevented or that a response was initiated on detection such that anything other than transient effects of a DDoS attack were avoided.

Estonia's Russian minority: Around 330,000 of Estonia's 1.3 million inhabitants are ethnic Russians.[37] Many more have Russian as their first language. The existence of such a significant Russian-speaking demographic comprised of citizens with Russian heritage was seen by Russia as an opportunity to energise and engage activists as well as their political and community representatives. The parliamentary vote to relocate the Tallinn monument caused both conventional protests and violent political activity. However, it remains to be seen to what extent these populations are a reliable resource for Russia to cause divisions between citizens of Estonia. It was reported that in the March elections, "[less than 1% of voters have said that they thought of the issue of the monument when making their choice [of which party to vote for]."[38] Despite the arrest of one individual, it does not seem that Estonian citizens or residents became spontaneously involved in either side of the cyber attack.

Threats

Use of hijacked resources, criminal networks with smart command and control: Cyber threats are known to have the capacity to cause massive disruption to the modern economy.[39] However, despite much hyperbole on 'electronic Pearl Harbors,' no significant and coherent cyber attacks occurred until Estonia was targeted in 2007. The ability for attacks to be effective without significant risk of attribution or retribution was new. This was achieved in a way that did not involve hacking or malware directed at the target, but leveraged the direction of massive amounts of internet traffic at target sites from hijacked computers (so-called 'zombie' computers) around the world.

When many computers are linked together and attempt to access or send vast amounts of data to target websites, they overwhelm those target systems with requests. This leads to the unavailability of those targets, whose information security personnel have to take measures to block the electronic addresses of the sending computers. When many computers are being used, this is a difficult task. Security personnel also noticed that when counter-measures were effective, the botnets were "actually throttling their attack rate,"[40] and when filters were removed, attacks "contained built-in intelligence to use its available bandwidth effectively," indicating that the attacks could not have been conducted by individuals, but that organised and automatic tools were being employed.[41] Estimates vary as to how many botnet computers were involved – some state 1-2 million;

[35] Aviram Jenik, "Cyberwar in Estonia and the Middle East," *Network Security* 4 (April 2009): 6, *https://doi.org/10.1016/S1353-4858(09)70037-6*

[36] Former White House cyber-security advisor Howard Schmidt cited in Larry Greenemeier, "Estonian Attacks Raise Concern Over Cyber 'Nuclear Winter'," 24 May 2007, *https://www.informationweek.com/estonian-attacks-raise-concern-over-cyber-nuclear-winter/d/d-id/1055474?piddl_msgorder=*

[37] "Population by Ethnic Nationality," *Statistics Estonia*, 9 June 2017, *http://www.stat.ee/34278*

[38] Kadri Liik, "The 'Bronze Year' of Estonia-Russia Relations," *Estonian Ministry of Foreign Affairs Yearbook* (2007): 73, *http://vm.ee/sites/default/files/content-editors/web-static/053/Kadri_Liik.pdf*

[39] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: *RAND*, 2009), *https://www.rand.org/pubs/monographs/MG877.html*

[40] Steve Mansfield-Devine, "Estonia: What Doesn't Kill You Makes You Stronger," *Network Security* 7 (July 2012): 14, *https://doi.org/10.1016/S1353-4858(12)70065-X*

[41] Ibid.

one bank reportedly saw 82,000 targeting it alone.[42]

The combination of the use of what transpired to be 'professional' attackers from a criminal organisation known as the 'Russian Business Network'[43] and entry level users of DDoS tools meant that the latter could screen the former from media scrutiny and political action.

Disrupted information flow: By preventing access to many forms of information (newspaper websites, messaging, bank balances), this cyber attack struck at the heart of Estonia's technology-dependent economy where the unrestricted flow of information and data is vital. This threatened to have effects on the psychology of citizens and the confidence of businesses and investors.

By targeting "the websites of all government ministries […], and several political parties [… and] the parliamentary email server,"[44] access to critical functions was halted. Citizens were isolated from their government, unable to access services or receive key information on the situation from elected representatives and others. The Estonian government was unable to post press releases to update its citizens on events, as its 'public briefing room' was one of the first sites to be targeted.[45] The then US Homeland Security Secretary stated that the attack was "an actual threat to the national security and the ability of [the] Estonian government to govern its country."[46]

Effects

Aftermath of the cyber attacks: This DDoS attack caused significant disruption, cost, and embarrassment to Estonia. In addition, the physical disruption of supply lines meant that company orders were cancelled by Russian purchasers; goods failed to flow predictably and smoothly across borders, and messages and finance could not be transmitted to fulfil contracts. Government, businesses, and citizens who had enthusiastically adopted internet services were unable to access them reliably.

This cyber attack demonstrated the ability of the Russian Federation to inflict expensive, disruptive costs onto the state of Estonia without needing to draw on conventional and escalatory forms of military and political force. It sent a message that even a few hackers could cause asymmetric damage and weaken the Estonian population's confidence in their military and security structures.

Public opinion: Many Estonians were denied access to normal websites, web-based services, and the ability to email parliamentarians. Unable to access their finances, transfer or receive money, and otherwise conduct business, there were direct and opportunity costs to businesses. However, nearly half (over 49 per cent) of Estonians said in a survey that they were not affected by the cyber attacks.[47] Although many citizens were undoubtedly irritated by the disruption the attacks caused, they did not direct their anger towards the state and its inability to protect its citizens and economy from interference. In fact, polls showed that confidence in the government actually increased after the riots (from 53 per cent in 2006 to 66 per cent in 2007).[48] The

[42] Ibid.

[43] Bobbie Johnson, "Russian Hacker Gang Who 'Stole Millions from Citibank' under Investigation," *The Guardian*, 22 December 2009, *https://www.theguardian.com/technology/2009/dec/22/russian-hackers-citigroup-cyber-security*

[44] "Estonia Hit by 'Moscow Cyber War'," *BBC News*, 17 May 2007, *http://news.bbc.co.uk/1/hi/world/europe/6665145.stm*

[45] Steve Mansfield-Devine, "Estonia: What Doesn't Kill You Makes You Stronger," *Network Security* 7 (July 2012): 13, *https://doi.org/10.1016/S1353-4858(12)70065-X*

[46] Tom Espiner, "Estonia's Cyberattacks: Lessons Learned, a Year on," *ZDNet*, 1 May 2008, *http://www.zdnet.com/article/estonias-cyberattacks-lessons-learned-a-year-on/*

[47] Survey by the Estonian newspaper Postimees, in which 1,243 Estonians were questioned. Quoted in: Cyrus Farivar, "A Brief Examination of Media Coverage of Cyberattacks (2007-Present)," *CCDCOE*, *http://www.ccdcoe.org/publications/virtualbattlefield/13_FARIVAR%20Web%20War%20One.pdf*

[48] Hanneli Rudi, "Eesti elanikud usaldavad enim televisiooni," *Postimees*, 13 July 2007, *https://www.postimees.ee/1682645/eesti-elanikud-usaldavad-enim-televisiooni*

medium and long-term effects were about national resilience, with short term effects essentially minimal.

The protests about the relocation of the war memorial (including a riot where one individual died and many were injured) undoubtedly hardened attitudes and prejudices of some Estonians from non-Russian and Russian-speaking heritages. The arrest of an Estonian with Russian heritage in connection with one cyber attack added to this. An opinion poll showed that 82 per cent of ethnic Estonians approved of Prime Minister Ansip's handling of the Bronze Soldier removal, whereas 84 per cent of the Russian-speaking population disapproved.[49] However, the cyber attacks certainly did not cause any popular pressure to reverse the decision to move the Tallinn monument.

Short- and long-term government response: This attack targeted important aspects of national security, but only used a DDoS attack methodology: this was relatively easily understood and countered (with assistance), thereby reducing the likelihood of a repeat offence causing a comparable amount of disruption and cost in the future.

Estonia, working with its own Computer Emergency Response Team (CERT), its European counterpart, and NATO CERTs and others began to identify the sources of attack, so that this unwanted web traffic could be blocked. Intelligence agency warnings about a potential cyber attack anticipated interference around the time of parliamentary elections, but this did not occur and defences and awareness remained heightened.

Supported by international and regional bodies, Estonia exploited an "informal small network of [its] Internet security community"[50] and was thus able to constitute an agile, dynamic, effective defence to the cyber attacks which meant that the extent of disruption and scale of cost was limited. Consequently, the malign effects on civil society, economic life, and political climate were very small. In addition, a 'Cyber Defence League' was established as a result of the attack which forms part of the Kaitseliit (a reserve formation with 16,000 members in total[51]) that would be activated in any future eventuality.

Ultimately the medium and long-term effects of this attack were highly detrimental to the attacker, as the resilience, capability, and capacity of Estonia, neighbouring Baltic and other states and international organisations (e.g. NATO) grew after being exposed to this real and sophisticated threat to national competitiveness and stability.

Within a year of the attacks, the Estonian Ministry of Defence drafted a national cyber security strategy, which was implemented in May 2008. Along with enhancing Estonia's "defensive posture," work was undertaken to strengthen the "international legal framework" around cyber attacks, increase international cooperation with the goal being "to protect the global cyber system."[52] In May 2008, the NATO Co-operative Cyber Defence Centre of Excellence – which had been planned since 2003 – was established in Tallinn, Estonia's capital.

[49] Mirjam Mäekivi, "Küsitlus: eestlased toetavad, muulased taunivad Ansipi tegevust," *Postimees*, 7 May 2007, *https://www.postimees.ee/1658021/kusitlus-eestlased-toetavad-muulased-taunivad-ansipi-tegevust*

[50] Steve Mansfield-Devine, "Estonia: What Doesn't Kill You Makes You Stronger," *Network Security* 7 (July 2012): 15, *https://doi.org/10.1016/S1353-4858(12)70065-X*

[51] Estonian Defence League (Kaitseliit), accessed on 22 January 2018: *http://www.kaitseliit.ee/en/edl*

[52] William C. Ashmore, "Impact of Alleged Russian Cyber Attacks," *Baltic Security & Defence Review* Volume 11 (2009): 10.

CONCLUSIONS

This first significant cyber attack caused some disruption and cost to Estonia, but was never intended to cause irreversible and lasting damage. It was first and foremost an act of communication. The intended message was that the Russian Federation had the capabilities to effectively isolate a state by disrupting the flow of data such as financial transfers, news, email, etc. This isolation could be initiated with no warning and be impossible to out-manoeuvre.

A related strategic message could be related to the target state's inability to attribute responsibility, severely impeding the ability of the affected state or others (e.g. NATO) to launch targeted counter-measures. The criminal 'Russian Business Network,' a smokescreen generated by the actions and statements of patriotic, self-organised, and spontaneous actors, was assisted with sophisticated state-led reconnaissance targeting information. Given the widespread lack of understanding of cyber risk, the media and many politicians were unable to immediately see through this deception.

The cyber attacks and complementary economic measures against Estonia fit into a pattern of behaviour by the Russian Federation. First, a symbolic act was used as the organising point to enable the attribution of cyber attacks to spontaneously-acting uncoordinated individuals. Whether in the case of the Tallinn memorial, or passing a law in Lithuania prohibiting the display of Soviet symbols, attacks are carefully monitored to ensure that although damage is caused and costs are imposed, no thresholds for reprisals (e.g. triggering of NATO's Article V) are crossed. It is thus crucial to have not only an understanding of the adversary's weapons and tools, but also of their mode of operation. Does the adversary carefully plan targeted offensives, or does it operate more reactively and opportunistically, exploiting opportunities as they materialise?

The Estonian government's handling of the crisis proved to be adequate, especially regarding the novelty of apparently non-state actors attacking 'soft' civilian targets. However, in trying to determine state attribution, some Estonian government officials might have been almost too focused on the attack's technical components (such as attempting to trace individual IP addresses). In the last ten years, NATO and the EU have come a long way in understanding how different sources of assessment come together, and how best to determine the degree of *probability*. Governments have grown more mature in dealing with cyber attacks. Governments learned that response options are not limited to military (for instance triggering Article V) and legal measures, but that broader diplomatic tools and a consistent international response can have more impact.

Recommendations

Prepare and look for no notice, sophisticated attack. Although significant in terms of scale and with the impact of being the first such attack mounted with no warning, "from a technical perspective, the thrust and sophistication of the attacks were relatively modest, if not low compared to global standards, even in 2007."[53]

[53] Andreas Schmidt, "The Estonian Cyberattacks," January 2013, 11, *https://www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks*

The fact that disruption was caused and not swiftly remediated indicated a lack of preparation on the part of the Estonian state, particularly their ability to swiftly detect, block, and manage the consequences of a relatively primate attack. It is recommended:

- That governments, NATO, and private sector infrastructure providers plan for plausible cyber, blended, and hybrid attacks that could occur at no notice and be extremely challenging to counter.

- That governments, NATO, private sector infrastructure providers and others share information on potential hostile reconnaissance of systems and people in order to prevent or at least achieve early warning of forthcoming attacks.

- That due consideration is given to the use of cyber (or other) attacks as distractions whilst other attacks, pre-placement or reconnaissance is conducted.

Prepare to neutralise efforts to deny attribution. The ability of the Russian Federation to dismiss the DDoS cyber attack as the actions of patriotic, uncoordinated and spontaneous individuals could have been prevented, by building a strong and credible narrative that, in fact, only state-sponsored actors could plausibly have been behind the attack. By broadening the cyber literacy of communicators (e.g. press officers, heads of news, government ministers), media, politicians, and civil society would be able to prevent effective plausible deniability. It is recommended:

- That efforts are undertaken to deepen and broaden the understanding of cyber risks across society.

- That strategic communications and related functions are improved to enable governments to effectively counter claims which deny accountability. This would combine education to the public about the attack's nature and the likelihood that relatively few adversaries would wish to undertake such an attack.

- That the exploitation of internal political conflict by adversaries should be anticipated: altering the scheduled timing of, say, the relocation of a monument disrupts attack plans and enables undermines adversary claims that events were the spontaneous action of un-coordinated groups and individuals.

Coordination and mutual aid brings benefits. The effective management and recovery of this DDoS cyber attack has undoubtedly enhanced the resilience and preparedness of Estonia. In turn, Estonia has been able to support other countries develop or enhance their anticipation of and readiness to deal with such threats. NATO provided critical input and continues to undertake research and delivery of guidance and support that will assist all NATO and PfP (Partnership for Peace) states. However, it would be better if such capability development were not caused by crises. It is recommended:

- That the insight gained from the effective response and recovery to such incidents is used to help states ensure that they prepare for credible threats in advance of them occurring.

- That NATO members and others prepare for no notice events which quickly escalate to being a severe or even critical challenge to the management and sustainability of a state.