JOURNAL OF ADVANCED FORENSIC SCIENCES

ISSN NO: 2692-5915

Research

DOI: 10.14302/issn.2692-5915.jafs-20-3601

A Critical Evaluation of the Estonian Cyber Incident

Donald L. Buresh, Ph.D., JD, LL.M.[1,*]

[1]Cybersecurity and Policy Department, Morgan State University, Baltimore, Maryland

Abstract

This paper evaluates the effect of the Estonian cyber incident on Estonia, Russia, the United States, the European Union, and the North Atlantic Treaty Organization, also known as NATO. The paper employs the Valeriano and Maness criteria for evaluating a cyber incident critically. The article asks how did the Estonian cyber incident come to pass, what were the foreign policy and international relationship effects, what was the impact on Estonia, and how did Estonia react to the attack. The essay concludes that the Estonian cyber incident was a catalyst, prompting the nations listed herein to address the effects of cyber-attacks, and then search for acceptable solutions.

Corresponding author: Donald L. Buresh, Ph.D., J.D., LL.M. 3115 Enoch Avenue, Zion, Illinois 60099 Telephone: 847-872-1659.

Keywords: Cyber-attack, Cyber terrorism, Digital terrorism, Estonian cyber-attack

Received: Oct 22, 2020 **Accepted:** Oct 27, 2020 **Published:** Nov 03, 2020

Editor: Barbara Kelemen, Central European Institute of Asian Studies (SK).

Introduction

The purpose of this paper is to analyze the Estonian cyber incident of 2007 critically using the Valeriano and Maness criteria[1]. The analysis will focus on answering the following four questions:

- How did the Estonian incident come about?
- What was the foreign policy and international relations contest of the Estonian attack?
- What was the impact of the attack on Estonia? and
- What was the reaction to the incident by Estonia?[2]

Because there were five parties involved in the incident – Estonia, Russia, the United States, the European Union, and NATO – the answer to the second question is divided into three parts, (1) the relationship between Estonia and the United States, the European Union, and NATO, (2) the relationship between Estonia and Russia, and (3) the relationship between the United States and Russia. The paper concludes by pointing out that the Estonian attacked resulted in better political relations between Estonia and the West, the publication of the Tallinn Manual, while Russia became further isolated from the Western powers.

How Did the Estonian Incident Come About?

The Estonian cyber-attack started on Friday, April 27, 2007, and finished on Friday, May 18, 2007, continuing for three weeks[3]. The attack was triggered by the decision of the Estonian government to move a Soviet World War II memorial of a Bronze Soldier from central Tallinn, the capital city of Estonia, to a military cemetery[4]. During holidays related to World War II, Russian Estonians commemorated their losses by placing flowers on the site[5]. These events increasingly provoked hostile actions against the Estonian government by the Russian government and Russian media, where the protests in the streets quickly morphed into riots[6]. The Estonian embassy came under siege, and the Estonian ambassador to Russia was physically harassed.[7] Estonians had almost universal access to the Internet, where the government had promoted information technology to expand the ability of Estonian citizens to communicate with their government and vice versa[8]. By 2001, the Estonian government had become virtually paperless[9].

The cyber attackers employed the following four methods against the Estonian government and Estonian companies and institutions:

- Distributed Denial of Service ("DDoS") attacks;
- Website defacement; and
- Data Name Servers ("DNS") attacks;
- Mass email comment spam.[10]

First, the attacks from April 27 to April 29 involved defacing government websites, where these attacks were reasonably clear-cut, employing the ping command[11]. However, over time, malformed web queries were used against government and media sites[12]. The second phase began on May 04, involving penetrating and precise attacks against these sites and data-name servers that employed botnets, where the attacks came from proxy servers located in foreign countries[13]. The second wave lasted from May 09 to May 11[14]. In Russia, May 09 is Victory Day, a national holiday, celebrating the defeat of Nazi Germany in World War II[15]. During this phase, phase, the DDoS attacks were amplified by 150 percent against government websites[16]. Hansapank, the largest Estonian bank, was also impacted by the DDoS attacks[17].

During the third wave, 85,000 Estonian computers were hijacked, where the third wave occurred from noon until midnight on May 15[18]. The attack on the SEB EestiÜhispank website, Estonia's second-largest commercial bank, lasted for approximately 1.5 hours for Estonian customers and much longer for customers outside the country[19]. On May 18, or during the fourth wave, both government and banking websites suffered from DDoS attacks[20]. The attacks were traced to computers in 178 different countries and were probably politically motivated by people who followed instructions on Russian-language websites[21]. The second phase of the episode seemed to be controlled from a central location, but only a few individuals acknowledged responsibility for the attacks[22]. The Russian government denied any involvement in the cyber-attacks[23].

The cyber-attack noticeably affected the whole Estonian economy because Estonian institutions heavily relied on information and communications technology infrastructure[24]. Banks, media companies, government institutions, and small to medium businesses were affected[25]. Communication with public administrators was significantly impeded along with the information flow to other countries, where one side-effect was that legitimate Internet traffic was congested[26]. On a technical level, Estonia, along with the European Union ("EU") and the North Atlantic Treaty Organization ("NATO"), worked together to combat this attack[27]. In the end, public awareness was magnified, Estonia began cooperating with other nations to prevent such attacks in the future, thereby raising international awareness of cyber-criminal activity[28]. The result of the episode was that countries became aware that cyber-attacks have global consequences with the possibility of affecting multiple regions and nations[29].

What Was the Foreign Policy and International Relations Contest of the Estonian Attack?

In attempting to appreciate the foreign policy and international implications of the Estonian cyber-attack, it is necessary to list the players. Based on the information above, the parties involved directly or indirectly were Estonia, Russia, the European Union, NATO, and the United States[30]. Mathematically, there are ten possible relationships to consider[31]. However, from a practical perspective, this number can be drastically reduced because several of the relationships are similar. For example, Estonia's relationship to the United States, the EU, and NATO can be analyzed as a single relationship because (1) NATO is led by the United States, and (2) the EU is an ally of the United States. Estonia's relationship with Russia is another possibility because Estonia is a Baltic state that borders Russia, and according to Valeriano and Mannes[32], rivalries may exist between Estonia and Russia. Finally, there is the relationship between the United States and Russia to contemplate. Even though the United States and the European Union are separate sovereign entities, and NATO is a non-government organization, their relationship is more likely related to the relationship between the United States and Russia.

Estonia and the United States, the European Union, and NATO

The primary effect of the Estonian cyber-attack was that Estonia drew closer to the West, particularly the United States, the EU, and NATO[33]. Mansel aptly pointed out that the country went from Estonia to *E-stonia*[34]. According to McGuinness, the government of Estonia has established a voluntary Cyber Defence Unit[35]. These individuals are trained by the Estonian Ministry of Defence, donating their free time to protecting their country by practicing what procedures to follow if a utility or an Internet service provider was the victim of a cyber-attack[36]. After the Russian annexation of the Crimea in 2014, on the weekends, 25,000 Estonian volunteers dress up in fatigues, practicing their shooting skills[37].

Another major international event that brought Estonia closer to the United States, the EU, and NATO were the creating of the *Tallinn Manual on the International Law Applicable to Cyber Warfare*

("Tallinn Manual")[38]. It was written by the Tallinn-based *NATO Cooperative Cyber Defence Centre of Excellence* ("CCDCE") by an international group of approximately twenty experts[39]. According to Schmidt, in the latter part of 2009, the CCDCE assembled an international group of legal scholars and practitioners to write a manual that dealt with interpreting international law in the context of cyber operations and cyber warfare[40]. It was the first time that the international community comprehensively and authoritatively addressed cyber operations and cyberwar with the desire to bring order to these highly complex legal issues[41].

The result of these efforts was that Estonia drew closer to the West, and the West embraced Estonia[42]. Another consequence of the Estonian attack was the increased political distance between Russia and the United States, the EU, and NATO[43]. In other words, the Estonian attack further strained the relations between the United States and Russia (Valeriano & Maness, 2015)[44]. This will be discussed later in this paper.

Estonia and Russia

According to Valeriano and Maness, the purpose of the Estonian cyber-attack was to punish Estonia for disrespecting Russian culture, history, and identity by removing the Bronze Soldier from central Tallinn to a military cemetery[45]. At the beginning of World War II and during the post-war period, Estonia became a satellite state of the Union of Soviet Socialist Republics

("USSR"). Thus, it makes sense that when the USSR dissolved, and Estonia received its independence, there would be significant animosity between the two sovereigns[46]. It should also be remembered that during pre-World War II, there was a substantial number of ethnic Russians that lived in Estonia[47]. After the war, Estonia was ruled by Moscow via Russian-born Estonian governors. They were from families of native Estonians residing in Russia, having later obtained their education in the Soviet Union during the Stalinist era[48]. Many of these individuals had fought in the Red Army under the guise of the Estonian Rifle Corps[49]. Even so, only a few spoke the Estonian language[50].

According to Valeriano and Maness, the dispute about the Bronze Soldier began in 1991 when Estonia, like many other satellite states, cast off the Soviet yoke[51]. Like Latvia and Lithuania, the two other Baltic states, Estonia, viewed the Soviet annexation into the USSR after World War II, trading one oppressive regime (Nazi Germany) for another (the USSR)[52]. Given that in 2007 seven percent of ethnic Russians lived in Estonia, it was not surprising that these individuals perceived the movement of the Bronze Soldier as an affront to their Russian identity and to the millions of Russians that died during World War II while freeing the world from Nazi oppression[53]. As a significant power and as a permanent member of the United Nations Security Council, one could anticipate that Russia would be offended by Estonia relegating the Bronze Soldier to a seemingly unknown location[54].[55] According to Valeriano and Maness, it is not astonishing that Russia reacted, or even overreacted, in a manner to protect its perceived honor[56]. What was startling was that Russia engaged in cyber action as a retaliatory response[57].

The United States and Russia

According to Stadnik, US-Russian cyber relations desires to answer the following two questions:

- Can the United States or Russia change the cybersecurity discussion in another country without committing a cyber-attack; and
- Do shifts in the discourse between the two power promote changes in foreign policy towards cyber-norms? [58]

Ashmore observed that the high profile Estonian attack thrust cybersecurity from the domain of Internet magazines into the mainstream media[59]. In the short-run, the attack advanced the perception of a new Cold War between the United States and Russia and between Russia and former Soviet satellites[60]. The episode also demonstrated that NATO, the EU, and even the United Nations ("UN") had inadequately prepared for preventing cyber-attacks[61].

At issue is that there is scant evidence indicating that the Russian government was involved in the attack[62,63]. Even so, the circumstantial evidence does suggest that the Russian government was probably behind or support the attack[64]. When countries or organizations are opposed to each other, a cyber-attack to influence the other party may be a viable option[65]. This rule seems to be correct, with one glaring exception – the relationship between the United States and China[66]. According to Valeriano and Maness wrote that only in this instance is a cyber-attack met with diplomacy by the United States rather than a cyber response[67].

On November 18, 2019, a United Nations committee passed a Russia-backed cybercrime resolution by a vote of 88 to 58, with 34 countries abstaining[68]. The resolution was sponsored by Russia,

Belarus, Cambodia, China, Iran, Myanmar, Nicaragua, Syria, and Venezuela, and was entitled, *Countering the use of information and communications technologies for criminal purposes*[69]. Unfortunately, the United States was disappointed with the decision[70].

The resolution created terms of reference for a future worldwide cybercrime treaty[71]. According to Sherman and Reynolds, hacking attacks, privacy violations, or identity thefts are not the primary concern of the document[72]. The idea behind the proposal is to make it easier for nations to cooperate in repressing political dissent[73]. Although the ramification of the vote is that China and Russia are becoming quite adept in traversing international politics via the UN, the effect on the US-Russian relationship is that the Russian government is taking steps to curb the blatant use of the Internet for political purposes.[74]

In contrast, according to Collier (2019), twenty-seven (27) nations expressly agreed that countries should adhere to international law regarding basic rules concerning cyber behavior[75]. Some signatories include the Five Eyes intelligence alliance (the United States, the United Kingdom, Australia, New Zealand, and Canada) and other major European nations, Colombia, Japan, and South Korea[76]. The agreement stated that it is acceptable to engage in cyber espionage among nations, but attacking civilian infrastructure or providing a country with an economic advantage is objectionable[77].

If the United States and other Western nations (including Japan and South Korea) can overcome their suspicion of Russia and China, the long-term effect of the Estonian attack could be greater cooperation between the two superpowers, their allies, and non-aligned states. Without an international cyber framework, cybercriminals will probably continue to operate successfully, profiting from their activities[78].

Thus, it appears that the Estonian attack may be the catalyst for future cooperation among the United States, Russia, and even China[79]. With diplomacy, a sense of urgency may not necessarily be a precious commodity, but what is essential is that the need for cyber rules is becoming increasingly evident. A synthesis between the American perspective on international cyber regulations and the Russian-Chinese view on cyber laws may be closer than some people think. Time will tell.

What Was the Impact of the Attack on Estonia?

According to Valeriano and Maness, the short-run monetary impact on Estonia was a loss of US $750 million in business and government revenues[80]. The Estonian government was hampered in conducting normal business operations or providing government services to its citizenry[81]. Estonia experienced another impact when NATO did not react thoughtfully while the attack occurred[82]. Rid observed that the long-term result of the incident was that Estonia successfully acquired from NATO permanent cybersecurity agency in Tallinn, the *Cooperative Cyber Defense Centre of Excellence[83]*. Although one should remember that the Centre was created before the Estonian incident, the cyber-attack assured that the Centre would, after that, become critical to NATO operations[84].

Finally, during the Estonian cyber-attack, there was the real possibility that Estonia would have invoked Article 5 of the NATO Charter, thereby yanking other NATO states into the fray and potentially causing a crisis in conventional foreign policy[85]. Fiedler (2013) insightfully observed that when other nations are drawn into a conflict, the chances of success decline dramatically. The reason is that calmer minds may be cast to the wayside[86]. According to Valeriano and Maness, it is possible that Estonia over- reacted, but with no precedent to guide the nation, the Estonian response may have, after all, been reasonable.[87]

What Was the Reaction to the Incident by Estonia?

According to Valeriano and Maness, after the cyber-attack ended, Estonians felt violated and vulnerable[88]. A Saar Poll indicated that 65 percent of all Estonians believed that cyber incidents were the greatest threat to this small Baltic state[89]. In comparison, 55 percent of Estonians thought that foreign intervention threatened Estonian sovereignty[90]. According to Valeriano and Maness, the cyber-attack did little or no damage beyond a loss of time and a perceived loss of security[91]. Essentially, the threat of a conventional conflict was negligible[92]. The real impact is that Estonia is now considered a cybersecurity hub, where Tallinn, the capital of Estonia, has hosted the International Conference of Cyber Conflict at least five times[93].

Although Estonia could have prompted NATO to engage in a tit-for-tat response, at the end of the day, it was Russia that was chastened as a disruptor of the international order[94]. There is a question regarding Russia's culpability, but it is probably correct to say that the Russian government could have stopped the attack[95]. Quite likely, the sophistication of the attack caught the attention of the Russian Federal Security Service ("FSB"), the successor to the Komitet Gosudarstvennoy Bezopasnos ("KGB"), and the American Central Intelligence Agency ("CIA")[96]. The Estonian targets were hit with surgical precision, pointing to Russian government involvement[97]. To naïvely state that the cyber-attack was an amateur effort challenges the reasonable mind[98]. The scope, precision, and organization of the cyber-attack seem to support the conclusion that the attack possessed government support[99]. Finally, the cyber-attack was comprehensive because of the Estonian response, and not because the attack was organized at the beginning of the conflict[100].

Conclusion

In conclusion, the Estonian cyber incident was a significant cyber-attack that did not lead to a kinetic conflict[101]. It is also an important milestone because the attack led parties in the East and the West to a better understanding of cyber conflict and its ramifications. The *Tallinn Manual* was created in response to the Estonian cyber-attack[102]. Finally, even though the major powers cannot currently agree on how to address cyber conflicts, both the United States and its allies, together with China and Russia, seem to be seeking ways to mitigate cyber conflict. Over time, a synthesis will most likely occur, where the meshing of the two perspectives may yield a cohesive whole. It is only a matter of time.

References

1. B. VALERIANO, & R. C. MANESS, CYBER WAR VERSUS CYBER REALITIES: CYBER CONFLICT IN THE INTERNATIONAL SYSTEM (Oxford University Press 2015).
2. Id.
3. E. Tikk, E., K. Kaska, & L. Vihul, International cyber incidents: Legal considerations, CCDCOE, 2010, https://ccdcoe.org/publications/books/legalconsiderations.pdf.
4. Id.
5. Id.
6. Id.
7. Id.
8. Id.
9. Id.
10. D. L. Buresh, Does digital terrorism really exist? Journal of Advanced Forensic Sciences, 1(1), 2020, https://openaccesspub.org/jafs/article/1367.
11. Id.
12. Id.
13. Id.
14. Id.
15. Id.
16. Id., supra 3.
17. Id.
18. Id.
19. Id.
20. Id.
21. Id.
22. Id.
23. Id.
24. Id., supra 10.
25. Id.
26. Id.
27. Id.
28. Id.
29. Id.
30. Id., supra 1.
31. J. M. GEORGE, & G. R. JONES, UNDERSTANDING AND MANAGING ORGANIZATIONAL BEHAVIOR (Addison-Wesley Publishing 1996). Specifically, the number of relationships = (the number of parties * (the number of parties -1)) / 2 or = (5 * 4) / 2 = 10.
32. Id., supra 1
33. D. McGuinness, How a cyber attack transformed Estonia, BBC News, April 27, 2017, https://www.bbc.com/news/39655415.
34. T. Mansel, How Estonia became E-stonia, BBC News, May 16, 2013, https://www.bbc.com/news/business-22317297.
35. Id., supra 33.
36. Id.
37. Id.
38. Id., supra 3.
39. TALLINN MANUAL STAFF, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Cambridge University Press 2013).
40. M. N. SCHMITT (GEN. ED.), TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Cambridge University Press 2013).
41. Id.
42. Id., supra 1.
43. Id.

44. Id.

45. Id.

46. J. Hilden, & D. J. Smith, D. J., The Baltic States and their region: New Europe or old? Slavic Review, 65 (3), 2007, https://www.researchgate.net/publication/312413056_The_Baltic_States_and_Their_Region_New_Europe_or_Old/citation/download.

47. Id.

48. R. HUMPHREY, R. MILLER, & E. A. ZDRAVOMYSLOVA (EDS.) (2003), BIOGRAPHICAL RESEARCH IN EASTERN EUROPE: ALTERED LIVES AND BROKEN BIOGRAPHIES (Ashgate Publishing. 2003).

49. Id.

50. Id.

51. Id., supra 1.

52. Id.

53. Id.

54. UNSC Staff, United Nations Security Council, United Nations, n.d., https://www.un.org/securitycouncil/content/current-members

55. Id., supra 1.

56. Id.

57. Id.

58. I. Stadnik, US-Russian relations in cybersecurity: The constructivist dimension. European Conference on Cyber Warfare and Security, July 01, 2019, https://search.proquest.com/openview/c910f8c8f8cc4779c9c055ce60ec6d12/1?pq-origsite=gscholar&cbl=396497.

59. W. C. Ashmore, Impact of alleged Russian cyber attacks, School of Advanced Military Studies. United States Army Command and General Staff College. Fort Leavenworth, Kansas, August, 2009, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-027.pdf.

60. Id.

61. Id.

62. Id.

63. Id., supra 1.

64. Id., supra 59.

65. Id.

66. Id., supra 1.

67. Id.

68. J. Sherman, & M. Reynolds, The UN passed a Russia-backed cybercrime resolution. That's not good news for Internet freedom, The Washington Post, December 04, 2019, https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom/.

69. Id.

70. Id.

71. Id.

72. Id.

73. Id.

74. Id.

75. K. Collier, 27 countries sign cybersecurity pledge with digs at China and Russia, CNN Politics, September 23, 2019, https://www.cnn.com/2019/09/23/politics/united-nations-cyber-condemns-russia-china/index.html.

76. Id.

77. Id.

78. Id., supra 59.

79. Id., supra 10.

80. Id., supra 1.

81. Id.

82. J. HEALEY, *A FIERCE DOMAIN: CONFLICT IN CYBERSPACE 1986-2012* (Cyber Conflict Studies Association 2013).

83. T. RID, *CYBERWAR WILL NOT TAKE PLACE* (Hurst & Company Publishing 2013).

84. Id.

85. Id., supra 1.

86. J. D. Fiedler, *Bandwidth cascades: Escalation and pathogen models for cyber conflict diffusion*, Small Wars Journal, June 19, 2013, http://smallwarsjournal.com/jrnl/art/bandwidth-cascades-escalation-and-pathogen-models-for-cyber-conflict-diffusion.

87. Id., supra 1.

88. Id.

89. Saar Poll Staff. (2013, October). *Public opinion and national defence*, Ministry of Defence of Estonia, October, 2013, http://www.kaitseministeerium.ee/files/kmin/nodes/13918_Public_Opinion_and_National_Defence_2013October.pdf.

90. Id.

91. Id., supra 1.

92. Id.

93. ICCC Staff, *International Conference on Cyber Conflict*, NATO Cooperative Cyber Defence Centre for Excellence, August 04, 2012, http://www.ccdcoe.org/cycon/

94. Id., supra 1.

95. Id.

96. Id.

97. Id., supra 1.

98. Id., supra 10.

99. Id.

100. Id.

101. Id., supra 1.

102. Id., supra 39.