OpenAccessPub

Journal of Advanced Forensic Sciences

ISSN: 2692-5915

DOI: 10.14302/issn.2692-5915.jafs-21-3930

Opinion Artic

Freely Available Online

Russian Cyber-Attacks on Estonia, Georgia, and Ukraine, Including Tactics, Techniques, Procedures, and Effects

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

[1]Morgan State University

Corresponding author:

Donald L. Buresh, Ph.D., JD, LL.M. Morgan State University

Keywords:

Cyber-Attack Tactics, Cyber-Attack Techniques Cyber-Attack Procedures, Cyber-Attack Effects Estonian Cyber-Attack, Georgian Cyber-Attack Ukrainian Cyber-Attack

Received: Aug 11, 2021

Accepted: Aug 14, 2021

Published: Aug 19, 2021

Abstract

The purpose of this essay is to compare and contrast the cyber-attacks on Estonia, Georgia, and Ukraine, including tactics, techniques, procedures, and effects. The paper states that none of the models will probably be repeated. The thesis is that cyber-attacks will change as technology changes. In other words, past cyber-attacks operations, particularly in Estonia, Georgia, and Ukraine, are not good predictors of future cyber-attack activity.

Introduction

This paper aims to look at the cyber-attacks of Estonia, Georgia, and Ukraine in light of future attacks. The issue is whether cyber attacks in years to come will resemble the attacks that occurred in Estonia, Georgia, and Ukraine, or will future attacks be based on new technologies that are currently emerging or in development. The cyber-attacks of Estonia, Georgia, and Ukraine are discussed in detail from the perspective of what occurred and what was learned. The thesis that is presented herein is that cyber-attacks will change and evolve as technology becomes more and more pervasive in everyday life. It is proposed that the cyber-attacks in Estonia, Georgia, and Ukraine are relatively poor predictors of future cyber-attacks.

Russian Cyber-Attacks

The Russian cyber-attacks that are

OPEN ACCESS

©2021 Donald L. Buresh This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and build upon your work non-commercially.

discussed include the Estonian, Georgian, and Ukrainian cyber-attacks. Each attack is analyzed in terms of its tactics, techniques, procedures, and effects. The measures taken to counter the cyber-attacks and lessons learned from the cyber-attacks are also highlighted in some detail.

Estonian Cyber-Attack

The Estonian cyber-attack began on Friday, April 27, 2007, and ended on Friday, May 18, 2007. The attack lasted for three weeks.[1] The attack was precipitated by the Estonian government's decision to move a Soviet World War II memorial of a Bronze soldier two meters high from central Tallinn, the capital city of Estonia, to a military cemetery.[2] During World War II-related holidays, individuals commemorated their losses by placing flowers on the Tallinn site.[3] However, over time, these events increasingly provoked hostile actions against the Estonian government.[4] The movement of the statute was countered by intense opposition by the Russian government and Russian media, where protests in the streets quickly devolved into riots, the Estonian embassy went under siege, and the Estonian ambassador to Russia was physically harassed.[5]

There was almost universal access to the Internet in Estonia, where the government promoted information technology to increase the administrative ability to foster communications between Estonian citizens and their government and became virtually paperless in 2001.[6] The cyber attackers employed three methods against the Estonian government and Estonian institutions. The attacks consisted of Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS) attacks, website defacement, attacks against Data Name Servers (DNS), and mass email comment spam.[7] The attacks of April 27 through April 29 consisted of defacing government websites using the straightforward *ping* command.[8] However, as time went by, malformed web queries were employed against the sites of the government and media outlets.[9]

In the second phase of the attack, the first wave began on May 04, involving intense and precise attacks against websites and data name servers by using botnets, routing the attacks from proxy servers in other countries.[10] While the second wave lasted from May 09 through May 11, it should be remembered that in Russia, May 09 is the national holiday, Victory Day, signifying the defeat Nazi Germany in World War II.[11] The DDoS attacks increased by 150 percent against government websites during the second phase, lasting from May 09 to May 10.[12] Although the Estonian government was the primary victim of the attack, Hansapank, the largest Estonian bank, was also affected by the DDoS attacks.[13]

The third wave involved the hijacking of 85,000 Estonian computers, taking place from noon until midnight on May 15.[14] The website for SEB Eesti Ühispank, Estonia's second-largest commercial bank, lasted about 1.5 hours for Estonian customers and extended more for customers outside the country.[15] On May 18, or the fourth wave, both government and banking websites experienced DDoS attacks.[16] The source of the attacks was traced to computers in 178 different countries.[17] The attacks were politically motivated by individuals who were following instructions on Russian-language websites.[18] The second phase of the attack appears to be centrally controlled.[19] There were only a few individuals that took credit for the attacks.[20] The Russian government denied involvement in the cyber-attacks.[21]

The cyber-attack had a noticeable effect on the Estonian economy, affecting commerce, industry, and governance that relied on information and communications technology (ICT) infrastructure.[22] Bank, media companies, government institutions, and small to medium businesses were all affected.[23] The societal effect was that communication to public administration was significantly hampered along with the information flow to other countries.[24] A side-effect was that was the legitimate Internet traffic was clogged.[25] There was substantial technical response employed, with international cooperation from the European Union (EU) and the North Atlantic Treaty Organization (NATO).[26] There was also increasing public awareness as Estonia

OPEN ACCESS

©2021 Donald L. Buresh This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and build upon your work non-commercially.

worked with other countries to bring cybercriminals to justice.[27]

The lessons learned are manifold. The Estonian cyber-attack raised international awareness that cyber-attacks were new forms of criminal activity in an information society.[28] The attacks accentuated the need for mutual criminal assistance on an international level.[29] The challenge was to appreciate that cyber-attacks have international implications affecting one country and a global region or even the whole planet itself.[30]

Georgian Cyber-Attack

The Georgian cyber-attack began on Friday, August 08, 2008, and ended on Thursday, August 28, 2008, and the attack lasted for three weeks.[31] The attack was precipitated by an armed conflict between the Russian Federation and the country of Georgia over South Ossetia.[32] In 2008, the Internet had a low penetration rate of 7 percent of the population.[33] At the time, Georgia was not heavily dependent on IT infrastructure, but there were limited options to connect to the Internet via land routes, where the connections that did exist heavily depended on Russia.[34]

There were several methods employed in the Georgian cyber-attack. DoS and DDoS were involved, including distributing malicious MS batch scripts whose instructions exploited Structured Query Language (SQL) vulnerabilities.[35] Websites were also defaced, and email was used for targeting spamming attacks.[36] The targets were the President of Georgia, the Georgian Parliament, Ministries, and the local government of Abkhazia. Financial institutions such as banks were also affected by the attacks.[37] Although there was little or no evidence linking the Russian government or state organizations to the attacks, it was thought that Russian hackers were the culprits.[38] In essence, there is no conclusive proof as to who was behind the DDoS or defacement attacks.

The effects of the Georgian attacks were limited because of the kinetic military conflict between Russia and Georgia.[39] Because of the lack of communication technology in Georgia at the time, the transmission of information to the outside world was constrained, particularly during the beginning of the conflict.[40] Primary communications operations were severely affected because most of the Georgian communications lines passed through Russia.[41] Internet services had to be relocated to servers outside the country.[42] National Community Emergency Response Team (CERT) assistance came from other countries to help alleviate the interruption of Internet service.[43] The Georgian academic center CERT mitigated the attack by assuming the role of the Georgian national CERT at the time of the attack.[44] There was a state-mandated blockage on Russian websites to control information flow and free up bandwidth where services to servers were relocated to other countries.[45] The national CERTs from other countries were thus involved in helping Georgia overcome the cyber-attack.[46]

One of the significant lessons learned from the Georgian cyber-attacks was the applicability to the Law of Armed Conflicts (LOAC).[47] The right of a country to employ force against another state depends on the actions of the other state.[48] The remedy must be proportionate to the threat and the harm incurred.[49] The problem with the Georgian cyber-attack was that it was difficult to estimate the direct effects of the attacks.[50] Because the Georgian population was not highly dependent on Internet services, the cyber-attacks were not sufficiently serious to result in severe economic damage or human suffering.[51] Thus, the application of the LOAC to the Georgian cyber-attacks seems problematic at best and irrelevant and immaterial at worst.[52] The challenges are that new approaches are needed to provide effective legal remedies, and that continued national information communication technologies are essential.[53]

Ukrainian Cyber-Attack

On December 23, 2015, Prykapattyapblenergo, a Ukrainian regional electricity distribution company,

OPEN ACCESS

©2021 Donald L. Buresh This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and build upon your work non-commercially.

stated that the service outages experienced by its customers were because of a third party's illegal entry into the company's computer and supervisory control and data acquisition (SCADA) systems.[54] The outage began at 3:35 PM local time.[55] Seven 110 kilovolt (kV) and twenty-three 35 kV substations were disconnected from the Ukrainian power grid for three hours.[56] The cyber-attack affected other portions of the distribution power grid, forcing the company to switch to manual mode.[57]

The Ukrainian news agencies conducted interviews and concluded that a foreign government had remotely controlled the SCADA electrical distribution system.[58] It was originally estimated that the outage only affected 80,000 customers.[59] However, it was later discovered that the electrical distribution grids for Chernivtsioblenergo and Kyivoblenerogo were affected. [60] In total, approximately 225,000 customers lost power due to the attack.[61] These cyber-attacks in Ukraine were the first attacks that were publicly acknowledged to have resulted in power outages.[62]

There were a variety of capabilities demonstrated by the Ukrainian attacks, including spear-phishing emails, variations on Black Energy 3 malware, and altering Microsoft Office documents that contained the malware.[63] The attack harvested credentials and information to gain admission to the Ukrainian ICT.[64] The attackers advanced two SCADA hijack approaches, the first one was a custom hijack, and the other was an agnostic hijack.[65] The attackers were successful in employing them across different types of SCADA/DMS implementations.[66] The attackers showed a desire to target field devices at substations, write custom malicious firmware, and ensure that specific devices were inoperable.[67]

It is not clear why these three oblenergos were targeted. Lee et al. gave the following possible decision factors.[68]

- Standard systems and configurations;
- Impact duration estimates;
- Existing capabilities would achieve the desired results;
- Risk-level was reasonable; and
- Access to act within the environment.

The lessons learned are legion. The spear-phishing employed social engineering techniques to target the Ukrainian oblenergos need to safelist extensively, identifying users that are given the specific privilege, service, mobility, access, or recognition.[69] Because *Black Energy 3* was used, user passwords should be changed periodically, data exfiltration and controlling access is critical, and two-factor authentication with user tokens should be applied.[70]

Attacks Most Likely to Occur in the Future

The purpose of this section of this essay is to discuss the likelihood of using the Estonian, Georgian, and Ukrainian cyber-attacks as models for future attacks. The paper points out that the Estonian and Georgian cyber-attacks share a familiar *modus operandi*, whereas the Ukrainian cyber-attack is either a special attack, a test attack, or possibly an attack by non-government actors. The reason is that the Estonian and Georgian cyber-attacks lasted for approximately three weeks, while the Ukrainian cyber-attack transpired for merely three hours. The difference in duration could be indicating an alternative explanation.

Estonian and Georgian Cyber-Attacks

The Estonian and Georgian cyber-attacks share several common characteristics. Both cyber-attacks used DoS and DDoS attacks, defacement of websites, and attacks on DNS.[71] Both attacks lasted for approximately three weeks.[72] The attacks occurred within 16 months, and both attacks were precipitated by the remembrance of a past war or an actual war.[73] At the time, Estonia had a highly developed Internet infrastructure, whereas the opposite was true in Georgia.[74]

In projecting whether these two cyber-attacks

OPEN ACCESS

©2021 Donald L. Buresh This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and build upon your work non-commercially.

would be good models for future attacks, the problem with such a prediction is that the technology employed is ten or more years old. Cell phones were present in the 2007-08 timeframe, but their sophistication at the time was a far cry from current technology.[75] The Internet-of-Things (IoT) was in its infancy.[76] The machines that instigated the cyber-attacks were likely either computer towers or notebooks. Sophisticated computers inside automobiles, televisions, refrigerators, microwaves, and gas and electric meters outside a home that use the Internet were virtually unknown a decade ago.[77] All of these devices are now candidates for bots to be used in future cyber-attacks.[78] Thus, based on the evidence above, the cyber-attacks of the future will probably not resemble the cyber-attacks that occurred in Estonia and Georgia.[79,80,81].

Ukrainian Cyber-Attack

As an example of future cyber-attacks, the December 2015 cyber-attack in Ukraine has serious credibility issues. First, in February 2014, the Ukrainian Euromaidan Revolution of 2014 occurred nearly two years before the Ukrainian cyber-attack.[82] The parties to the revolution that overthrew the existing government included the Euromaidan protestors, the Euromaidan militants (Sotnia), and the Right Sector, a Ukrainian neo-Nazi group.[83] At the time, the revolution appeared to be a neo-Nazi revolution, thrusting the Right Sector into political power.[84] The Russian people were adamantly against the new Ukrainian government because the 20 Soviet citizens died during World War II, defeating Nazi Germany.[85] The citizens of Crimea voted overwhelmingly to secede from Ukraine.[86] in fear that the new government would institute the ethnic cleansing of Russians in the peninsula.[87] The Eastern regions of Donbas and Luhansk also seceded from Ukraine because most of its citizens were either Russians or of Russian descent.[88] The government of Ukraine felt that the citizens of Crimea, Donbas, and Luhansk had illegally seceded from the country and that Russia had instigated the secession.[89] Thus, when the opportunity arose, it is reasonable to suggest that blaming Russia for the power outage was a way to cast dispersions on the country's northern neighbour.

Second, the electrical outage only lasted for three hours.[90] In the United States, it is not uncommon for power outages to last for three hours or more, mainly when a variety of events causes an equipment failure.[91] This author experienced a power outage for four days while living in Massachusetts after an ice storm.[92] In other words, a three-hour power outage could have been caused by a variety of reasons, including equipment failure or incompetence, not merely a cyber-attack by the Russian Federation. This is not to say that the Russian government or Russian citizens did not engage in a cyber-attack against Ukraine. The power outage could have been a testbed for future cyber-attacks.[93] Instead, this alternative explanation is mentioned to point out that alternative reasons are possible and maybe probable.

Third, unlikely, there is a possibility that the revolutionary Ukrainian government caused the power outage. On February 27, 1933, the German Reichstag burned to the ground because of arson.[94] One month earlier, Hitler was made Chancellor by von Hindenburg.[95] The fire was blamed on Marinus van der Lubbe, an unemployed Dutch construction worker who the police arrested because he was outside the building possessing firelighters.[96] He was also panting and sweating.[97] Van der Lubbe was tried for the arson and executed.[98] Hitler used the burning of the building as an excuse to pass The Enabling Act of 1933, assigning all legislative power to Hitler and his ministers, thereby permitting Hitler to control the German political process.[99] Hitler then proceeded to eliminate the Communists from German politics.[100]

In contrast, Hett argued that Hitler and the German Nazis could have caused the burning of the Reichstag to gain political power.[101] Hett observed that in the previous election, the Nazis had lost seats in the Reichstag.[102] To secure more power, Hitler may have used arson to abandon the constitution of the Weimar

OPEN ACCESS
©2021 Donald L. Buresh This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and build upon your work non-commercially.

Republic.[103] With the burning embers of the Reichstag not yet extinguished, Hitler arrested 5,000 people, primarily communists.[104] The result was the 12-year reign of the Third Reich.[105].

The Right Sector, a Ukrainian political party, is a neo-Nazi group that has Third Reich roots.[106] There is a possibility that the Ukrainian government used the power outage as an excuse to blame the Russian Federation for a cyber-attack, thereby garnering international support for the new Ukrainian government.[107] What is peculiar about the power outage is that it only lasted for three hours.[108] If it were indeed a Russian cyber-attack, the attack would probably have continued for more than a mere few hours, but then again, the attacks could be an effort by the Russian government, even if it is somewhat lackluster, to prevent Ukraine from joining the European Union.[109] Western media have claimed that the power outage was a cyber test conducted by the Russians Federation.[110] If so, the account would have to explain the short duration of the power outage. One possibility is that the Ukrainian cyber-attack was conducted by Russian hackers who were not affiliated with the Russian government.[111] It is also possible that Right Sector hackers attacked the Ukrainian government facilities while spoofing their URL attacking addresses to make it appear that the Russian government was involved in the cyber-attack, but there is seemingly no proof to this theory. It is indeed far more likely that Estonia and Georgia were attacked by the Russian Federation even though the Russian government denied any involvement in the attacks.[112] After all, the Estonian and Georgian attacks lasted for three weeks.[113] There are several alternative explanations and too many political axes to grind by Ukraine and the Western powers to conclude positively that the power outage was a Russian Federation cyber-attack.[114] The Russian Federation may have had little to nothing to gain by instigating a three-hour cyber-attack against the three oblenergos, except collecting the data from a cyber-test.[115] However, when considering the potential adverse effects on world opinion, Russia had a lot to lose if it was determined to be the perpetrator of the attacks.[116] Thus, the short-lived cyber-attacks of oblenergos may not have originated in Russia and are probably not a good model for future international cyber-attacks.[117] It appears that a cyber-test of this magnitude, if it was indeed a test, need only be conducted once and not repeated.[118]

A Glimpse into the Future

The short response to whether the three cyber-attack models discussed above is likely to be repeated in the future is none of the above.[119] The reason is that the answer depends on the date and time of the attack and the technology that is employed by the attack.[120] For example, if a cyber-attack were to occur now, there would be little or no change in technology.[121] The attack would probably very closely resemble past attacks because the cyber-attack would use existing available technology, such as fax machines, printers, video conference systems, security cameras, door access systems, and heating, ventilation, and cooling systems.[122] There would be almost no change in the availability of the IoT and their controlling computer systems.[123] Thus, a cyber-attack could resemble the Estonian, Georgian, or Ukrainian attacks, depending on the existing hardware and software employed by the attackers and available at the target site.

However, if we move forward five, ten, or 20 years, the situation dramatically changes. The technology in this future period will probably be entirely different from the technology around us today.[124, 125] First, there is the IoT. Smart devices are being marketed and sold to consumers at a rapid pace.[126] IoT will pervasively dominate our economy in the next five to ten years.[127] These devices will probably possess less than adequate security features because security will likely be brushed aside in a rush to market, while cybercriminals will note this situation and probably exploit it.[128]

Stuxnet and its variations will probably play a dramatic role in future cyber-attacks.[129] When the United States government used Stuxnet a decade ago to disrupt Iranian centrifuges, a physical machine was involved that

OPEN ACCESS

©2021 Donald L. Buresh This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and build upon your work non-commercially.

stopped working correctly.[130] The child or grandchild of Stuxnet could be employed to modify the actions of physical devices such as automobiles, televisions, refrigerators, or microwave ovens.[131] These devices could be programmed by malware to stop functioning or even to explode.[132] A car is the most potentially dangerous of the machines mentioned because it is large, heavy, and moves quickly.[133] With sophisticated computers inside controlling the operation of an automobile, cars could be employed to run people over or even explode in crowded areas.[134] A Stuxnet-like virus that infected a vehicle could be programmed to affect specific vehicles that would injure or kill particular individuals, where the attack occurs in an automobile assembly plant or while driving.[135] When this type of cyber-attack occurs, a kinetic response of some sort may be entirely appropriate under certain conditions, such as what happened when Archduke Ferdinand, the heir to the Austrian-Hungarian Empire, was the heir at the time to the Austrian-Hungarian Empire assassinated on June 28, 1914.[136]

When looking 20 years into the future, it is quite likely that human beings will be physically connected to the Internet via nanotechnology that is implanted into their bodies.[137] This technology could interact with human DNA, causing numerous issues.[138] For example, a cyber-attack could involve programming humans to perform actions that they normally would not do. A cyber-attack could circumvent human free will.[139] If the attack was sufficiently malicious, it might be possible to program humans to attack others or to do nothing when a defensive response would be appropriate. In this case, society could easily resemble a *Brave New World* or a *1984* society.[140,141]

Thus, a future cyber-attack depends on the date and time that the attack occurs and the technology involved. Without this information, it is probably impossible to predict what a future cyber-attack will resemble with any precision or accuracy. However, with this information, the only impediment to a precise and accurate prediction is the imagination of a sage or prophet. A prospective attacker will have no such limitation. They are already well aware that the future belongs to them.

References

1. Eneken Tikk, Kadri Kaska, & Liis Vihul, *International Cyber Incidents: Legal Considerations*, The NATO Cooperative Cyber Defence Centre of Excellence, (2010), *available at* https://ccdcoe.org/library/publications/international-cyber-incidents-legal-considerations/.
2. Id.
3. Id.
4. Id.
5. Donald L. Buresh, *A Critical Evaluation of the Estonian Cyber Incident*, 1 Journal of Advanced Forensic Sciences 2, 7-14, (November 03, 2020), DOI 10.14302/issn.2692-5915.jafs-20-3601.
6. Id.
7. Id.
8. Rain Otis, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, The Cooperative Cyber Defence Centre of Excellence, (n.d.), *available at* https://ccdcoe.org/uploads/2018/10/Otis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.
9. Id.
10. Id.
11. Id.
12. Eneken Tikk, Kadri Kaska, & Liis Vihul, *supra*, note 1.
13. Id.
14. Id.
15. Id.
16. Rain Otis, *supra*, note 8.
17. Eneken Tikk, Kadri Kaska, & Liis Vihul, *supra*, note 1.

©2021 Donald L. Buresh This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and build upon your work non-commercially.

18. Id.
19. Id.
20. Id.
21. Id.
22. Stephen Herzog, *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*, 4 JOURNAL OF STRATEGIC SECURITY 49-60, (Summer 2011), *available at* DOI: http://dx.doi.org/10.5038/1944-0472.4.2.3.
23. Emily Tamkin, *10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?*, FOREIGN POLICY, (July 2020), *available at* https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.
24. Id.
25. Id.
26. Id.
27. Id.
28. The Conversation Staff, *Cyber Attacks Ten Years On: From Disruption to Disinformation*, THE CONVERSATION, (April 26, 2017), *available at* https://theconversation.com/cyber-attacks-ten-years-on-from-disruption-to-disinformation-75773.
29. Id.
30. Id.
31. Eneken Tikk, Kadri Kaska, & Liis Vihul, *supra*, note 1.
32. Id.
33. Id.
34. Id.
35. Dancho Danchev, *Coordinated Russia vs Georgia Cyber Attack in Progress*, ZDNET, (August 11, 2008), *available at* https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/.
36. Id.
37. Id.
38. Id.
39. Lesley Swanson, *The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian -Georgian Cyber Conflict*, 32 LOY. L.A. INT'L & COMP. L. REV. 303, (2010), *available at* http://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=1010&context=ilr.
40. Id.
41. Id.
42. Id.
43. Id.
44. Eneken Tikk, Kadri Kaska, & Liis Vihul, *supra*, note 1.
45. Id.
46. Id.
47. Sarah P. White, *Understanding Cyberwarfare: Lessons from the Russia-Georgia War*, MODERN WAR INSTITUTE AT WEST POINT, (March 20, 2018), *available at* https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf.
48. Id.
49. Id.
50. Id.
51. Eneken Tikk, Kadri Kaska, & Liis Vihul, *supra*, note 1.
52. Id.
53. Id..
54. Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED, (March 03, 2016), *available at* https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.
55. Id.
56. Id.

OPEN ACCESS

©2021 Donald L. Buresh This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and build upon your work non-commercially.

57. Id.
58. Robert M. Lee, Michael J. Assante, & Tim Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid* Electricity Information Sharing and Analysis Center, (March 18, 2016), *available at* https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf.
59. Id.
60. Id.
61. Id.
62. Id.
63. CPI Staff, *Black Energy Ukraine*, EU Cyber Direct: Cyber Policy Institute, (n.d.), *available at* https://eucyberdirect.eu/wp-content/uploads/2020/11/2015-black-energy-ukraine.pdf.
64. Id.
65. Kaspersky Staff, *BlackEnergy APT Attacks in Ukraine*, Kaspersky, (2021), *available at* https://www.kaspersky.com/resource-center/threats/blackenergy.
66. FireEye Staff, *Cyber Attacks on the Ukrainian Grid: What You Should Know*, FireEye, (2016), *available at* https://www.fireeye.kr/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf.
67. Id.
68. Robert M. Lee, Michael J. Assante, & Tim Conway, *supra*, note 58.
69. Id.
70. Id.
71. Eneken Tikk, Kadri Kaska, & Liis Vihul, *supra*, note 1.
72. Id .
73. Id.
74. Id.
75. Charles Arthur, The History of Smartphones: Timeline, The Guardian, (January 12, 2014), *available at* https://www.theguardian.com/technology/2012/jan/24/smartphones-timeline.
76. Keith D. Foote, *A Brief History of the Internet of Things*, DataVersity, (August 06, 2016), *available at* http://www.dataversity.net/brief-history-internet-things/.
77. Id.
78. Id.
79. Jack M. Germain, *The Future of Cybersecurity in 2021 and Beyond*, Tech News World, (January 16, 2021), available at https://www.technewsworld.com/story/the-future-of-cybersecurity-in-2021-and-beyond-87018.html.
80. Arnaud de Borchgrave, Cyber Threats and Information Security: Meeting the 21st Century Challenge (Csis Report) (Center for Strategic & Intl Studies May 21, 2001).
81. Chuck Brooks, *3 Key Cybersecurity Trends To Know For 2021 (and On ...)*, Forbes, (April 12, 2021), *available at* https://www.forbes.com/sites/chuckbrooks/2021/04/12/3-key-cybersecurity-trends-to-know-for-2021-and-on-/.
82. Andrey Kurkov, *Ukraine's Revolution: Making Sense of a Year of Chaos*, BBC News, (November 21, 2014), *available at* https://www.bbc.com/news/world-europe-30131108.
83. Id.
84. Jack Losh, *Ukraine Turns a Blind Eye to Ultrarightist Militia*, The Washington Post, (February 13, 2017), *available at* https://www.washingtonpost.com/world/europe/ukraine-turns-a-blind-eye-to-ultrarightist-militia/2017/02/12/dbf9ea3c-ecab-11e6-b4ff-ac2cf509efe5_story.html?utm_term=.c688f9c2d870.
85. Id.
86. CBS News Staff, *Official Results: 97 Percent of Crimea Voters Back Joining Russia*. CBS News, (March 17,

©2021 Donald L. Buresh This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and build upon your work non-commercially.

2017), *available at* https://www.cbsnews.com/news/official-results-97-of-crimea-voters-back-joining-russia/. The vote by the citizens of Crimea was overwhelmingly in favor of becoming part of the Russian Federation. According to CBS NEWS, 97 percent of Crimean voters voted in favor of becoming part of the Russian Federation. The Crimean vote was apparently an excellent example of the self-determination of peoples, regardless of the lamenting of the American political class. For an example of their bemoaning, see, Steve Pifer, *Crimea: Six Years After Illegal Annexation*, BROOKINGS INSTITUTE, (March 17, 2020), *available at* https://www.brookings.edu/blog/order-from-chaos/2020/03/17/crimea-six-years-after-illegal-annexation/.

87. David M. Herszenhorn, *Crimea Votes to Secede from Ukraine as Russian Troops Keep Watch*, THE NEW YORK TIMES, (March 16, 2014), *available at* https://www.nytimes.com/2014/03/17/world/europe/crimea-ukraine-secession-vote-referendum.html.
88. CBS News Staff, *No End in Sight for Ukraine's Deadly, "Pointless War"*, CBS NEWS, (September 08, 2016), *available at* https://www.cbsnews.com/news/ukraine-war-russia-rebels-donbass-luhansk-donetsk-pointless-ceaseless/.
89. Id.
90. Robert M. Lee, Michael J. Assante, & Tim Conway, *supra*, note 58.
91. Heidi Moore, *Rush-Hour Power Outages Hit New York, LA and San Francisco*, LADDERS, (April 21, 2017), *available at* https://www.theladders.com/career-advice/power-outages-nightmare-commute.=
92. The ice storm occurred in Westford, Massachusetts in circa December 1997. The power was out for four days due to downed power lines.
93. Kim Zetter, *The Ukrainian Power Grid Was Hacked Again*, MOTHERBOARD, (January 10, 2017), *available at* https://motherboard.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report.
94. Loraine Boissoneault, *The True Story of the Reichstag Fire and the Nazi Rise to Power*, SMITHSONIAN MAGAZINE, (February 21, 2017), *available at* https://www.smithsonianmag.com/history/true-story-reichstag-fire-and-nazis-rise-power-180962240/.
95. Id.
96. Id.
97. Id.
98. Id.
99. Id.
100. Id.
101. BENJAMIN CARTER HETT, BURNING THE REICHSTAG: AN INVESTIGATION INTO THE THIRD REICH'S ENDURING MYSTERY (Oxford University Press 2014).
102. Id.
103. Id.
104. Id.
105. WILLIAM L. SHIRER, THE RISE AND FALL OF THE THIRD REICH: A HISTORY OF NAZI GERMANY (Simon & Schuster, Reissue ed. 2011).
106. Lev Golinkin, *Neo-Nazis and the Far Right Are On the March in Ukraine*, THE NATION, (February 22, 2019), *available at* https://www.thenation.com/article/archive/neo-nazis-far-right-ukraine/.
107. Donghui Park, & Michael Walstrom, *Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks*, THE HENRY M JACKSON SCHOOL OF INTERNATIONAL STUDIES: UNIVERSITY OF WASHINGTON, (October 11, 2017), *available at* https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.
108. Robert M. Lee, Michael J. Assante, & Tim Conway, *supra*, note 58.

OPEN ACCESS
©2021 Donald L. Buresh This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and build upon your work non-commercially.

109.Donghui Park, & Michael Walstrom, supra, note 107.

110.Kim Zetter, *supra*, note 54.

111.Donghui Park, & Michael Walstrom, supra, note 107.

112.Kim Zetter, *supra*, note 54.

113.Eneken Tikk, Kadri Kaska, & Liis Vihul, *supra*, note 1.

114.Donghui Park, & Michael Walstrom, supra, note 107.

115.Terry Gross, *Experts Suspect Russia Is Using Ukraine as a Cyberwar Testing Ground*, National Public Radio, (June 22, 2017), *available at* https://www.npr.org/2017/06/22/533951389/experts-suspect-russia-is-using-ukraine-as-a-cyberwar-testing-ground.

116.Id.

117.Id.

118.Id.

119.Jack M. Germain, *supra*, note 79.

120.Id.

121.David Taintor, & Danielle Zoellner, *New York Subway Hacked in Computer Breach Linked to China*, The Independent, (June 02, 2021), *available at* https://www.independent.co.uk/news/world/americas/crime/cyberattack-new-york-subway-china-b1858492.html.

122.Corey Nachreiner, *Breach of Rust: How Hackers Break in through Old Tech*, Industry Week, (March 19, 2019), *available at* https://www.industryweek.com/technology-and-iiot/article/22027329/breach-of-rust-how-hackers-break-in-through-old-tech.

123.Joe Tidy, *Colonial Hack: How Did Cyber-Attackers Shut Off Pipeline?*, BBC News, (May 10, 2021), *available at* https://www.bbc.com/news/technology-57063636.

124.Julian Jang-Jaccard, & Surya Nepal, *A Survey of Emerging Threats in Cybersecurity*, 80 Journal of Computer and System Sciences 5, 973-93, (August 2014), *available at* https://www.sciencedirect.com/science/article/pii/S0022000014000178/pdfft?md5=68a8ae049bb64caaa3557689e743cad5&pid=1-s2.0-S0022000014000178-main.pdf.

125.Staff Writers, *Hot Technologies in Cybersecurity*, Cyber Degrees, (April 29, 2021), *available at* https://www.cyberdegrees.org/resources/hot-technologies-cyber-security/.

126.Lauren Johnson, *Marketers Are Racing to Reach Rapidly Growing Audiences on Amazon's Alexa and Google Home*, AdWeek, (January 08, 2018), *available at* https://www.adweek.com/digital/marketers-are-racing-to-reach-rapidly-growing-audiences-on-amazons-alexa-and-google-home/.

127.UBS Staff, *Future of the Tech Economy: Investing Where Technology Meets Economy*, Union Bank of Switzerland, (June 2020), *available at* https://www.ubs.com/content/dam/static/noindex/wealth-management/cio/future-of-the-tech-economy-20200610.pdf?campID=DDL-CIOFUTUREOFTECHONOMY-EMAIL-GLOBAL-20200617-PDF.

128.Jon Gold, *A Lack of IoT Security Is Scaring the Heck Out of Everybody*, Network World, (May 31, 2017), *available at* https://www.networkworld.com/article/3198914/internet-of-things/a-lack-of-iot-security-is-scaring-the-heck-out-of-everybody.html.

129.Irving Lachow, *The Stuxnet Enigma: Implications for the Future of Cybersecurity*, Georgetown Journal of International Affairs 118–126, (2011), available at https://www.jstor.org/stable/43133820.

130.Jess David Ohlin, Kevin Govern, & Claire Finkelstein, Cyberwar: Law and Ethics for Virtual Conflicts (Oxford University Press 2015).

©2021 Donald L. Buresh This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and build upon your work non-commercially.

131. David Shamah, *Top Security Exec: Beware the 'Sons of Stuxnet'*, THE TIMES OF ISRAEL, (August 10, 2021), *available at* https://www.timesofisrael.com/top-security-exec-beware-the-sons-of-stuxnet/.

132. Lolita C. Baldor, *Stuxnet Virus Represents Dire Threat, Officials Say*, NBC NEWS, (November 17, 2010), *available at* https://www.nbcnews.com/id/wbna40238546.

133. Kevin Bullis, *Laws of Physics Persist: In Crashes, Big Cars Win*, MIT TECHNOLOGY REVIEW, (April 14, 2009), *available at* https://www.technologyreview.com/s/413018/laws-of-physics-persist-in-crashes-big-cars-win/.

134. Ruben Salvadori, *Here is how hackers can remotely take control of your car*, AOL.COM, (July 21, 2015), *available at* https://www.aol.com/article/2015/07/21/here-is-how-hackers-can-remotely-take-control-of-your-car/21212188/.

135. Lolita C. Baldor, *supra*, note 132.

136. James M. Lindsey, *TWE Remembers: The Assassination of Archduke Franz Ferdinand*, COUNCIL ON FOREIGN RELATIONS, (June 27, 2014), *available at* https://www.cfr.org/blog/twe-remembers-assassination-archduke-franz-ferdinand.

137. Chris Stein, *Meet the Humans with Microchips Implanted in Them*, CBS NEWS, (June 22, 2016), *available at* https://www.cbsnews.com/news/meet-the-humans-with-microchips-implanted-in-them/.

138. Id.

139. Christoph Lauterwasser (ed.), *Opportunities and Risks of Nanotechnology*, THE OECD INTERNATIONAL FUTURES PROGRAMME, (n.d.), *available at* https://www.oecd.org/science/nanosafety/37770473.pdf.

140. ALDOUS HUXLEY, BRAVE NEW WORLD (Chatto and Windus Publishers 1931).

141. GEORGE ORWELL, 1984 (Harcourt Brace Publishers 1949).

©2021 Donald L. Buresh This is an open access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and build upon your work non-commercially.