OPEN ACCESS
Freely Available Online

JOURNAL OF ADVANCED FORENSIC SCIENCES

ISSN NO: 2692-5915

Research

DOI: 10.14302/issn.2692-5915.jafs-20-3405

Does Digital Terrorism Really Exist?

Donald L. Buresh, Ph.D., J.D.[1,*]

[1]Touro University Worldwide

Abstract

This paper attempts to answer the question of whether digital terrorism, also known as cyberterrorism, exists. The paper defines terrorism both in the conventional and digital sense. It then gives a short history of conventional terrorism, dating back two thousand years and ending with the terrorist activities in several third-world nations. The essay then discusses digital terrorism, highlighting the Estonian, Georgian, and Ukrainian cyber-attacks. The work concludes that digital terrorism does indeed exist, but that the future is uncertain in the sense that future cyber-attacks will probably not resemble past attacks as the technology advances.

Corresponding author: Donald L. Buresh, Ph.D., J.D., 3115 Enoch Avenue, Zion, Illinois 60099 Telephone: 847-872-1659. Email: LoganSquareDon@sbcglobal.net

Keywords: Conventional terrorism, Cyber terrorism, Digital terrorism, Estonian cyber-attack, Georgian cyber-attack, Ukrainian cyber-attack

Received: Apr 25, 2020 **Accepted:** May 13, 2020 **Published:** May 25, 2020

Editor: Sunpreet Singh, Department of Mechanical Engineering, Lovely Professional University, Phagwara, Punjab 144411, India.

Definition of Terrorism

According to Merriam-Webster's Dictionary, terrorism is "the systematic use of terror especially as a means of coercion"[1]. Jenkins defined terrorism to be "the systematic use of violence to create a general climate of fear in a population and thereby to bring about a particular political objective"[2]. Terrorism is a tactic that has been practiced "by nationalistic and religious groups, by revolutionaries, and by armies, intelligence services, and police"[3]. Hoffman defined terrorism as an act of violence or the threat of violence that is employed in pursuing a political goal[4]. Richardson wrote that terrorism is an act that deliberately and violently targets civilians for political reasons[5]. According to Richardson, in dealing with terrorism, the point is not to rid the world of terrorism, but rather to manage and contain it so that its effects are mitigated[6]. Walzer observed that the purpose of terrorism is to deliberately and randomly kill innocent people to spread fear throughout the population with the intent of changing the behavior of political leaders[7]. Coady observed that the definition of terrorism could not be resolved because it is mainly polemical, ideological, and propaganda-oriented[8]. Finally, according to the United Nations Security Council ("UNSC") in Resolution 1566, terrorism is criminal act against civilians "committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons …"[9].

In contrast, digital terrorism, or cyberterrorism as it is also known, is a controversial term. Cyberterrorism can be narrowly defined as disruptive attacks by recognized terrorist organizations against computer systems with the intent of generating an alarm, panic, or the physical disruption of the information system, or it can be defined to encompass cybercrime[10]. Digital terrorism can be described as the intentional employment of computers, networks, andAccording to Merriam-Webster's Dictionary, terrorism is "the systematic use of terror especially as a means of coercion the Internet to create harm and damage in the promotion of personal objectives through hacking government systems, hospital records, or even national security programs such that an organization or country may end up fearing future digital attacks[11]. Similar to the definition of garden variety terrorism, the objective is political or ideological, where the idea is to disrupt the status quo and change the behavior of the leaders of organizations or nations[12].

Existence of Digital Terrorism

The question that this essay is attempting to answer is whether digital terrorism or what is commonly known as cyber terrorism exists. When questions regarding the existence of a notion are asked, the answer depends on its definition. According to the definitions of terrorism discussed above, the purpose of terrorism is to make individuals of an organization or a government fearful by disrupting the processes that operate within that organization or government or by killing or maiming those individuals[13]. The common ground between the definition of conventional terrorism and the definition of cyber terrorism is that both activities attempt to disrupt the processes of an organization or government[14]. The difference in the two definitions hinges on whether the killing and maiming of individuals are critical to the meaning of cyber terrorism[15].

If the killing and maiming of people is an inherent characteristic of cyber terrorism, there would be seemingly little or no difference between conventional terrorism and cyberterrorism. In cyber terrorism, the means of conducting the attack has shifted from a direct kinetic attack to a cyber-attack, where the kinetic effects are a consequence of the cyber-attack[16]. A significant difference between conventional terrorism and cyber terrorism is that the frequency of digital terrorist attacks dwarfs the rate of traditional terrorist attacks[17]. Digital terrorist attacks occur daily, where hundreds of thousands, if not millions of people are adversely affected by the offense[18]. See Table 1 for a sampling of the volume of people affected by data breaches or cyber-attacks just in the United States in 2019 and 2020[19].

In contrast to digital or cyber terrorism, conventional terrorist attacks are relatively infrequent. Most people are aware of the terrorist attack on the World Trade Center on September 11, 2001[20]. However, fewer people are aware of the 1993 attack on the World Trade Center, where six people were killed,and more

Table 1. Serious Data Breaches in 2019 and 2020

Organization	**Date**	**Individuals Affected**
550px	February 15, 2019	14.8 million
Antheus Technologies	March 11, 2020	81.6+ million
Ascension	January 23, 2019	24 million
Bodybuilding.com	April 22, 2019	9 million
CafePress	August 05, 2019	23 million
Capital One	July 29, 2019	100 million
Dow Jones	March 01, 2019	2.4 million
Dutch Government	March 11, 2020	6.9 million
Emuparadise	June 10, 2019	11 million
Facebook	December 19 2019	267 million
First American	May 25, 2019	885 million
Hostinger	August 25, 2019	14 million
Labcorp	June 04, 2019	7.7 million
LifeLabs	December 17, 2019	15 million
Marriott	March 31, 2020	5.2 million
Microsoft	January 22, 2020`	250 million
Quest Diagnostics	June 03, 2019	11.9 million
UniCredit	October 28, 2019	3 million
Wyze	December 30, 2019	2.4 million

than 1,000 people were injured[21]. In this attack, an explosion created a hole in the World Trade Center 200 feet by 100 feet and was several stories deep, causing the PATH station ceiling to collapse[22]. The cause of the explosion was a 1,200-pound bomb that was located in a Ryder truck, parked in a garage underneath the Center[23]. Fifty-thousand (50,000) people were evacuated from the World Trade Center because of the attack[24].

Another conventional terrorist attack occurred on March 11, 2004, where 191 people were killed, and more than 1,800 people were injured in Madrid, Spain[25]. Ten bombs located in backpacks and other small bags exploded on four commuter trains[26]. Still another attack occurred in Montrouge, a suburb of Paris, France where from January 07, 2015, to January 09, 2015, seventeen people were killed when Muslim terrorists attacked the headquarters of the magazine Charlie Hebdo because the magazine had recently published satirical cartoons about the Islamic prophet Mohammad[27]. Although these terrorist attacks occurred in America and Europe, conventional terrorist attacks are international, where no nation is seemingly immune. For example, there is the Moscow theater hostage crisis, also known as the 2002 Nord-Ost siege, where 40 armed Chechens seized the crowded Dubrovka Theater on October 23, 2002[28]. Because of the attack, there were approximately 900 hostages and 130 Russians that died[29]. Other conventional terrorist activities include the Bosnian genocide of 1992, the Rwandan genocide of 1994, and the on-going Boko Haram killings in Nigeria[30,31,32]. In China, it is difficult to verify the nature and magnitude of China's terrorism issues[33]. However, China does have a terrorism problem[34]. For example, on September 30, 2015, there was an explosion of 17 package bombs in the Guangxi Province that killed seven people[35]. Although not as frequent as digital terrorism, it appears that conventional terrorism is alive and well and active throughout the world.

Review of Conventional and Digital Terrorism

The word "terror" is derived from the Latin verb "tersere" which then evolved into the word "terrere"[36]. The word "tersere" is also the Latin root word for the English word "terrible"[37]. In the Middle Ages, the word became "terrour," and in modern times, the letter "u" was dropped, thereby arriving at the word "terror"[38].

Conventional Terrorism

Terrorism is a tactic and began thousands of years ago. During the 1st Century C.E., Jewish Zealots in Judea rebelled against Roman rule[39]. According to Josephus Flavius and Whiston, an extreme offshoot of the Zealots, known as the Sicarii ("dagger men"), targeted temple priests, Sadducees, Herodians, and other Jewish collaborators by stabbing them to death with short daggers that they hid underneath their cloaks[40]. On November 05, 1605, a group of conspirators that was headed by Robert Catesby tried to destroy the English Parliament when Guy Fawkes planted a large quantity of gunpowder beneath the Palace of Westminster[41]. The intent was to kill James I, then King of England, along with the members of both houses of Parliament, thereby restoring Catholicism to the kingdom[42]. The plot was uncovered, and all of the conspirators were killed. This terrorist attack is now known as the *Gunpowder Plot*[43].

During the French Revolution of 1789 and the years that followed before the reign of Napoleon Bonaparte, terrorism took on a whole new meaning. The Parisian Reign of Terror lasted from mid-1793 and ended with the fall of Maximilian Robespierre in July 1794[44]. It was a period where the French monarchy and nobilitywere systematically executed[45]. At the time, Paris was ruled by the Committee of Public Safety that directed mass executions with public purges of the nobility of individuals who were considered royalists[46]. It should be noted that the Constitution of the United States was ratified in 1789, the same year when the French Revolution began[47].

In Europe, there were the Revolutions of 1848, beginning in France in February of that year and spreading across the continent. These revolutions were fundamentally bourgeois revolutions with the goal of removing the old monarchical structures and creating independent and democratic nation-states[48]. They were an *ad hoc* series of revolutions across Europe, where the proponents were seen as terrorists by the ruling class[49]. The Paris Commune was a radical socialist government that ruled Paris from March 18, 1871, to May 28, 1871[50]. With the capture of Emperor Napoleon III in September 1870 during the Franco-Prussian War, the Second

French Empire collapsed, and the Third Republic began[51]. Paris was under siege for four months, and it was an opportunity for the French socialists to seize power in Paris[52]. Fortune did not favor the radical socialists, as the rest of France and the conquering Prussians perceived them to be terrorists[53]. When the Commune was overthrown, it was estimated that there were over 20,000 Commune causalities[54].

In August 1914, World War I broke out[55]. When the Kaiser's army beat the Russian army, and Czar Nicholas II sued for peace, the Germans returned Vladimir Ilyich Ulyanov, more commonly known as Vladimir Lenin, to Russia[56]. Lenin proceeded to organize the Communists in the country. In 1917, he played a leading role in the October Revolution, where the Bolsheviks overthrew the provisional government, which was formed after the Czar was ousted from power[57]. Lenin was a divisive individual who was perceived as a champion of socialism by his supporters and the founder of a repressive and authoritarian regime responsible for mass killings and political repression by his opponents[58].

After World War II ended in August 1945, it seemed that the world was tired of war[59]. The United Nations, the successor of the failed League of Nations, was founded on October 24, 1945, in San Francisco, California[60]. After experiencing two world wars in 20 years, the world seemed ready for peace[61]. In the 1950s and 1960s, the European powers that had colonies in Africa and other continents decided to make the fledglings fly[62]. One African nation after another received their independence[63]. The results of this effort were mixed. At times, the results were violent revolutions and terrorist attacks, typically along tribal lines[64]. These political upheavals and acts of terrorism have lasted for decades and are currently still occurring in several nations on the continent[65].

Digital Terrorism

The rise in cyber-terrorism paralleled the growth of the Internet in the 1990s[66]. With emerging information-based society, came the risks of cyber terrorists being able to damage data with computer attacks. From a psychological perspective, the word "cyberterrorism" combines the fear of violent actions with the fear of technology. The reason is that an unknown threat is perceived to be more powerful psychologically than a known threat, such as a terrorist bomb. After 9/11, the two fears of a violent attack and technology were merged into one idea – cyberterrorism. When the political dimension was added to the mix, the debate about national security reached a fever pitch, where al Qaeda was seen to be able to use technology to perpetrate nightmarish kinetic damage. The lack of reliable information, or more importantly, the plethora of misinformation, led to the hysteria that al Qaeda and Iraq were capable of employing cyber tools to disable American defenses. The result was an aggressive American policy to combat cyber warfare and cyber terrorism, where the FBI requested and obtained from Congress $4.5 billion for infrastructure security and the ability to hire over 1,000 cyber investigators. This call to action had all of the makings of a suave James Bond rolled into the geekish Bill Gates[67].

Through cyberterrorism against governments, private servers, networks, or other electronic devices, hackers can damage systems using viruses, worms, or Trojans, launching denial-of-service ("DoS") attacks, defacing websites, or even demanding that governments or companies pay substantial ransoms[68]. Examples of cyberterrorism include:

- Global terror networks that disrupt major sites by initiating public nuisances or stopping Internet traffic;
- International cyberterrorists accessing and then disabling or modifying signals to military technology;
- Cyberterrorists targeting critical infrastructure systems such as a water treatment plant or an electrical grid; or
- Cyberespionage that carried out by governments or private organizations to spy on intelligence communications[69].

Cyberterrorists can employ a variety of methods to attack a network. They may access a network or a server and then wait for an opportune time to strike[70]. A cyber terrorist could steal data rather than damage a network if the information is valuable[71]. For example, in 2015, it was reported that the Chinese stole security clearance information on 22.1 million Americans with security clearances, including employees, contractors, as

well as family and friends[72]. Viruses, worms, and other computer malware can jeopardize water supplies, transportation systems, power grids, critical infrastructure, and military systems[73]. For example, in Ukraine, a virus was discovered that disabled the country's power grid[74]. DoS attacks can be conducted against both governments and private companies[75]. For example, one of the more significant DoS attack as of this writing occurred in February 2018, where GitHub, public source code management service that is used by millions of software developers, experienced an incoming attack traffic rate of 1.3 terabytes per second[76]. Other forms of cyber-attacks include ransomware where computers are held hostage until a specified ransom is paid or phishing attacks where cybercriminals attempt to collect information through email and other means to commit identity theft[77]. Yet another type of cyber-attack can occur nations, particularly when the state actors are engaging in asymmetric warfare in furtherance of their own ends[78].

The defenses against cyberterrorism vary depending on the type of attack. The installation of effective anti-virus software, as well as periodically checking systems for the presence of malware, can effectively mitigate cyber-attacks[79]. Even so, constant vigilance is necessary as cybercriminals and cyberterrorists are continually developing new methods to thwart cybersecurity[80].

Examples of Digital Terrorism

In the past decade, there have been three significant cyberterrorism acts that have been extensively covered in the literature. They include the Estonian cyber-attack, the Georgian cyber-attack, and the Ukrainian cyber-attack. These examples were selected because the cyber-attacks affected large portions of the infrastructures of the countries under consideration. The examples reflect the magnitude of the harm that has occurred in the past, and can occur in the present and future.

Estonian Cyberattack

The Estonian cyber-attack began on Friday, April 27, 2007, and ended on Friday, May 18, 2007. The attack lasted for three weeks[81]. 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. During World War II-related holidays, individuals commemorated their losses by placing flowers on the Tallinn site. However, with time, these events increasingly provoked hostile actions against the Estonian government. The movement of the statute was countered by intense opposition by the Russian government and Russian media. Protests in the streets quickly devolved into riots. The Estonian embassy went under siege, and the Estonian ambassador to Russia was physically harassed[82].

In Estonia, there was almost universal access to the Internet. The government promoted information technology to increase the administrative ability to foster communications between Estonian citizens and their government. The Estonian government became virtually paperless in 2001[83].

The cyber attackers employed three methods against the Estonian government and Estonian institutions. The attacks consisted of DoS attacks, Distributed Denial of Service ("DDoS") attacks, website defacement, attacks against Data Name Servers ("DNS"), and mass email comment spam. The attacks of April 27 through April 29 consisted of defacing government websites. These attacks were reasonablystraightforward using the *ping* command. However, as time went by, malformed web queries were employed against the sites of the government and media outlets[84].

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. The second wave lasted from May 09 through May 11. In Russia, May 09 is national holiday Victory Day, signifying the defeat of Nazi Germany in World War II. During the second phase, the DDoS attacks increased by 150 percent against government websites, lasting from May 09 to May 10. Hansapank, the largest Estonian bank, was also affected by the DDoS attacks[85].

The third wave involved the hijacking of 85,000 Estonian computers, taking place from noon until midnight on May 15. The website for SEB EestiÜhispank, Estonia's second-largest commercial bank, lasted for

about 1.5 hours for Estonian customers and longer for customers outside the country. On May 18 or the fourth wave, both government and banking websites experienced DDoS attacks. The source of the attacks was traced to computers in 178 different countries. The attacks were politically motivated by individuals who were following instructions on Russian-language websites. The second phase of the attack appeared to be centrally controlled. There were only a few individuals that took credit for the attacks. The Russian government denied involvement in the cyber-attacks[86].

The cyber-attack had a noticeable effect on the Estonian economy, which affected commerce, industry, and governance that relied on information and communications technology ("ICT") infrastructure. Bank, media companies, government institutions, and small to medium businesses were all affected. The societal effect was that communication to public administration was significantly hampered along with the information flow to other countries. A side-effect was that the legitimate Internet traffic was clogged. There was substantial technical response employed, where international cooperation both from the European Union ("E.U.") and the North Atlantic Treaty Organization ("NATO"). There was also increasing public awareness as Estonia worked with other countries to bring cybercriminals to justice[87].

The lessons learned were manifold. The Estonian cyberattack raised international awareness that cyber-attacks were new forms of criminal activity in an information society. The attacks accentuated the need for mutual criminal assistance on an international level. The challenge was to appreciate that cyber-attacks have international implications affecting not only one country but also a global region or even the whole planet itself[88].

Georgian Cyberattack

The Georgian cyber-attack began on Friday, August 08, 2008, and ended on Thursday, August 28, 2008. The attack lasted for three weeks. The attack was precipitated by an armed conflict between the Russian Federation and the country of Georgia over South Ossetia. In 2008, the Internet had a low penetration rate of 7 percent of the population. At the time, Georgia was not heavily dependent on IT-infrastructure. There were limited options to connect to the Internet via land routes, where the connections that did exist heavily depended on Russia[89].

There were several methods employed in the Georgian cyberattack. DoS and DDoS were involved, including the distribution of malicious M.S. batch scripts whose instructions exploited Structured Query Language ("SQL") vulnerabilities[90]. Websites were also defaced, and email was used for targeting spamming attacks. 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. 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 culprit[91]. 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. 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. Main communications operations were severely affected because most of the Georgian communications lines passed through Russia. Internet services had to be relocated to servers outside the country. National Community Emergency Response Team ("CERT") assistance came from other countries[92].

The Georgian academic center CERT mitigated the attack. It assumed the role of the Georgian national CERT at the time of the attack. There was a state-mandated blockage on Russian websites to control the flow of information and to free up bandwidth. Services to servers were relocated to other countries. The national CERTs from other countries were involved in helping Georgia overcome the cyber-attack[93].

One of the significant lessons learned from the Georgian cyberattacks was the applicability to the Law of Armed Conflicts ("LOAC"). The right of a country to employ force against another state depends on the actions of the other state. The remedy must be proportionate to the threat and the harm incurred. The problem with the Georgian cyberattack was that it was difficult to estimate the direct effects of the attacks. Because the Georgian population was not highly

dependent on Internet services, the cyber-attacks were not sufficiently serious to result in serious economic damage or human suffering. Thus, the application of the LOAC to the Georgian cyberattacks seems problematic at best and irrelevant and immaterial at worst. The challenges are that new approaches are needed to provide effective legal remedies, and that continued national information communication technologies ("ICT") are essential[94].

Ukrainian Cyberattack

On December 23, 2015, Prykapattyapblenergo, a Ukrainian regional electricity distribution company, stated that the service outages experienced by its customers were because of a third party's illegal entry into company's computer and supervisory control and data acquisition ("SCADA") systems[95]. The outage began at 3:35 PM local time. Seven 110 kilovolt ("kV") and twenty-three 35 kV substations were disconnected from the Ukrainian power grid for three hours. The cyber-attack affected other portions of the distribution power grid, forcing the company to switch to manual mode[96].

The Ukrainian news agencies conducted interviews and concluded that a foreign government had remotely controlled the SCADA electrical distribution system. It was initially estimated that the outage only affected 80,000 customers. However, it was later discovered that the electrical distribution grids for Chernivtsioblenergo and Kyivoblenerogo were affected. In total, 225,000 customers lost power due to the attack. These cyber-attacks in Ukraine were the first attacks that were publicly acknowledged to have resulted in power outages[97].

There were a variety of capabilities that were demonstrated by the Ukrainian attacks, including spear-phishing emails, variations on *Black Energy 3* malware, as well as altering Microsoft Office documents that contained the malware. The attack harvested credentials and information to gain admission to the Ukrainian ICT. The attackers advanced two SCADA hijack approaches, the first one was a custom hijack, and the other one was an agnostic hijack. The attackers were successful in employing them across different types of SCADA/DMS implementations. The attackers showed a desire to target field devices at substations, write custom malicious firmware, and ensure that certain devices were inoperable[98].

It is not clear why these three oblenergoswere targeted. Lee et al gave the following possible decision factors:

- Common systems and configurations;
- Impact duration estimates;
- Existing capabilities would achieve the desired results;
- Risk level was reasonable; and
- Access to act within the environment[99].

The lessons learned are legion. The spear-phishing employed social engineering techniques to target the Ukrainian oblenergosneeds to whitelist extensively, identifying users that are given the specific privilege, service, mobility, access, or recognition. Because *Black Energy 3*was used, user passwords should be changed periodically. Data exfiltration and controlling access is critical. Finally, two-factor authentication with user tokens should be applied[100].

Findings, Conclusions, and the Future

The question originally posed by this essay was whether digital terrorism existed. The evidence presented above indicates not only that digital terrorism exists, but also that conventional terrorism is still rearing its ugly head. However, it is not the existence of digital terrorism, or more commonly known as cyberterrorism, that is the concern of both governments and individuals alike. Rather, the issue that seems to dominate the consciousness of society is: What will the next cyber-attack look like? Will it resemble the Estonian cyber-attack, the Georgian cyber-attack, or the Ukrainian cyber-attack? Will it be like when the Chinese stole security clearance information on 22.1 million Americans with security clearances? Will it be similar to the alleged Russian attack on the Democratic National Convention ("DNC") servers? Will it be comparable to the recent GitHub cyber-attack, where the site experienced an incoming attack traffic rate of 1.3 terabytes per second? Or, will the next major attack be so new and unique that organizational defenses will be helpless to prevent it, mitigate it, or minimize the damages? This is what concerns the public today.

The good news, or rather the short answer, is that very shortly any new attack will probably be analogous to one or more of the cyber-attacks discussed above. For example, if a cyber-attack were to occur tomorrow, there would be little or no change in the technology. The attack would probably very closely resemble past attacks. The cyber-attack would probably use existing available technology. The technology would likely be computer towers, computer notebooks, and cell phones. There would be almost no change in the availability of the Internet of Things ("IoT") (e.g., computers in automobiles, televisions, refrigerators, microwave ovens, etc.). Thus, a cyber-attack would probably be akin to previous attacks, depending on the existing hardware and software employed by the attackers and available at the target site.

However, in five, 10, or 20 years, the situation may dramatically change. The technology in this future period will probably be entirely different from the technology around us today. First, there is the IoT. Smart devices are being marketed and sold to consumers at a rapid pace[101]. (Johnson, 2018). The IoT will pervasively dominate our economy in the next five to 10 years. These devices will probably possess less than adequate security features because security concerns will likely be brushed aside in a rush to market[102]. Cyber attackers will probably note this situation and then exploit it.

Stuxnet and its variations will play a dramatic role in future cyber-attacks. When Stuxnet was used by the United States government a decade ago to disrupt Iranian centrifuges, a physical machine was involved that stopped working correctly[103]. The child or grandchild of Stuxnet could be employed to modify the actions of physical devices such as automobiles, televisions, refrigerators, or microwave ovens. These devices could be programmed by malware to stop functioning or even to explode. A car is by far the most potentially dangerous of the machines mentioned because it is large, heavy, moves quickly, and may contain a fairly large amount of gasoline, which is volatile[104]. With sophisticated computers inside controlling the operation of an automobile, cars could be employed to run people over, or even explode in crowded areas[105]. A Stuxnet-like virus that infected a car could be programmed to affect specific vehicles that would injure or kill particular individuals. When this type of cyber-attack occurs, under certain conditions, a kinetic response by a government may be entirely appropriate.

When looking 20 years into the future, human beings will probably be physically connected to the Internet via nanotechnology that is implanted into their bodies[106]. This technology could interact with human DNA, causing innumerable issues[107]. For example, a cyber-attack could consist of programming humans to perform actions that they normally would not do by circumventing human free will[108]. 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 *1984* society or a *Brave New World* society, particularly with the advent of social media and the dark web[109,110,111].

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

References

1. TERRORISM, MERIAM-WEBSTER DICTIONARY, (n.d.), available at https://www.merriam-webster.com/dictionary/terrorism.
2. J. P. Jenkins, Terrorism, Encyclopedia Britannica, n.d., available at https://www.britannica.com/topic/terrorism.
3. Id.
4. B. HOFFMAN, INSIDE TERRORISM (Columbia University Press 2006).
5. L. RICHARDSON, WHAT TERRORISTS WANT: UNDERSTANDING THE ENEMY, CONTAINING THE THREAT, (Random House Publishers 2007).
6. Id.

7. M. WALZER, ARGUING ABOUT WAR (Yale University Press 2004).
8. C. A. J. Coady, Terrorism, morality, and supreme emergency, 114 Ethics: An International Journal of Social, Political, and Legal Philosophy 4, 2004, available at https://www.journals.uchicago.edu/doi/abs/10.1086/383440?journalCode=et.
9. UNITED NATIONS SECURITY COUNCIL, RESOLUTION 1566, (2004), available at https://www.un.org/ruleoflaw/files/n0454282.pdf
10. D. Canetti, M. Gross, I. Waismel-Manor, A. Levanon, & H. Cohen, How cyberattacks terrorize: Cortisol and personal insecurity jump in the wake of cyberattacks, 20 Cyberpsychology, Behavior, and Social Networking 2 (February 01, 2017), available at https://www.liebertpub.com/doi/10.1089/cyber.2016.0338.
11. M. Rouse, Cyberterrorism, TargetTech (December 2017), available at https://searchsecurity.techtarget.com/definition/cyberterrorism.
12. Id.
13. See supra, notes 2 and 5.
14. See supra, notes 7 and 11.
15. G. Weimann, Cyberterrorism: How real is the threat? United States Institute of Peace (December, 2004), available at https://www.usip.org/sites/default/files/sr119.pdf.
16. Id.
17. Id.
18. J. Rey, Business cyber attack stop 4,000 per day: Your guide to ransomware, Cybersecurity (November 30, 2016), available at https://www.entrepreneur.com/article/284754.
19. SelfKey Staff, All data breaches in 2019 & 2020 – An alarming timeline, SelfKey (April 07, 2020), available at https://selfkey.org/data-breaches-in-2019/.
20. A. Taylor, 9/11: The day of the attacks, The Atlantic (September 08, 2011), available at https://www.theatlantic.com/photo/2011/09/911-the-day-of-the-attacks/100143/.
21. CNN Library, 1993 World Trade Center bombing fast facts, Cable News Network (February 10, 2019), available at https://www.cnn.com/2013/11/05/us/1993-world-trade-center-bombing-fast-facts/index.html.
22. Id.
23. Id.
24. Id.
25. CNN Library, Spain train bombings fast facts, Cable News Network (February 25, 2019), available at https://www.cnn.com/2013/11/04/world/europe/spain-train-bombings-fast-facts/index.html.
26. Id.
27. CNN Library, 2015 Charlie Hebdo attacks fast facts, Cable News Network (December 24, 2018), available at https://www.cnn.com/2015/01/21/europe/2015-paris-terror-attacks-fast-facts/index.html.
28. RT Staff, Russia mourns victims of deadly Nord-Ost theater attack, Russia Today (October 26, 2017), available at https://www.rt.com/russia/407865-russia-morns-victims-of-deadly/.
29. Id.
30. History.com Editors, Bosnian genocide, History.com (August 21, 2018), available at https://www.history.com/topics/1990s/bosnian-genocide.
31. History.com Editors, Rwandan genocide, History.com (October 01, 2018), available at available at https://www.history.com/topics/africa/rwandan-genocide.
32. T. McCoy, Boko Haram may have just killed 2,000 people: 'Killing went on and on and on', The Washington Post (January 09, 2015), available at https://www.washingtonpost.com/news/morning-mix/wp/2015/01/09/boko-haram-may-have-killed-2000-people-in-one-attack/?utm_term=.ed048bda8681.
33. M. S. Tanner, & J. Bellacqua, China's response to terrorism, CAN Analysis & Solutions (June 2016), available at https://www.uscc.gov/sites/default/files/Research/Chinas%20Response%20to%20Terrorism_CNA061616.pdf.
34. Id.

35. S. Tiezzi, 17 Mail Bombs Kill 7 in China's Guangxi Province, The Diplomat (October 01, 2015), available at https://thediplomat.com/2015/10/17-mail-bombs-kill-7-in-chinas-guangxi-province/.
36. J. Fine, Political and philological origins of the term 'terrorism' from the ancient near east to our times, 46 Middle Eastern Studies 2, at 271-288 (April 06, 2010), available at https://www.tandfonline.com/doi/abs/10.1080/00263201003619927.
37. Id.
38. Id.
39. G. Chaliand, The history of terrorism: From Antiquity to al Qaeda (University of California Press 2007).
40. Josephus Flavius (author), & Whiston, W. (translator), Josephus: The complete works (Thomas Nelson Publishers 1998).
41. S. Adams, The Gunpowder Plot: Terror and toleration, History Today (November 11, 2005), available at https://www.historytoday.com/archive/gunpowder-plot-terror-and-toleration.
42. Id.
43. Id.
44. T. Carlyle, The French Revolution: A history (Modern Library Publishers 2002 [1837]).
45. Id.
46. Id.
47. History.com Editors, This day in history: June 21. History.com (July 28, 2019), available at https://www.history.com/this-day-in-history/u-s-constitution-ratified.
48. M. Rapport, 1848: Year of revolution (Basic Books Publishers 2008).
49. Id.
50. T. March, The history of the Paris Commune of 1871 (Macmillan & Company 1896).
51. Id.
52. Id.
53. Id.
54. B. Anderson, In the world-shadow of Bismarck and Nobel, 28 New Left Review II (July-August, 2004), available at https://newleftreview.org/II/28/benedict-anderson-in-the-world-shadow-of-bismarck-and-nobel.
55. B. W. Tuchman, The guns of August (Macmillan Publishing 1962).
56. Id.
57. Id.
58. C. Hill, Lenin and the Russian Revolution (Pelican Books 1971).
59. See supra, note 9.
60. Id.
61. Id.
62. D. Birmingham, The Decolonization of Africa (Routledge Press. 1995).
63. Id.
64. Id.
65. See supra, note 32.
66. See supra, note 15
67. Id.
68. See supra, note 11.
69. Id.
70. Id.
71. Id.
72. E. Nakashima, Hacks of OPM databases compromised 22.1 million people, federal authorities say, The Washington Post (July 09, 2015), available at https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm_term=.079a63b0e398.
73. See supra, note 11.
74. E. Weise, Malware discovered that could threaten electrical grid, USA Today (June 12, 2017), available at https://www.usatoday.com/story/tech/news/2017/06/12/malware-discovered-could-threaten-electrical-grid/102775998/.
75. See supra, note 11.
76. Cloudflare Staff, Famous DdoS attacks | The largest

DdoS Attacks of all time, Cloudflare, n.d., available at https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/.

77. See supra, note 11.
78. L. QIAO, & X. WANG, UNRESTRICTED WARFARE (Echo Point Books and Media. 1999).
79. See supra, note 11.
80. Id.
81. E. Tikk, K. Kaska, & I. Vihul, International cyber incidents: Legal considerations. CCDCOE, 2010, available at https://ccdcoe.org/publications/books/legalconsiderations.pdf.
82. Id.
83. Id.
84. Id.
85. Id.
86. Id.
87. Id.
88. Id.
89. Id.
90. Id.
91. Id.
92. Id.
93. Id.
94. Id.
95. R. M. LEE, M. J. ASSANTE, & T. CONWAY, ANALYSIS OF THE CYBER ATTACK ON THE UKRAINIAN POWER GRID (Electricity Information Sharing and Analysis Center March 18, 2016).
96. Id.
97. Id.
98. Id.
99. Id.
100. Id.
101. L. 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/.
102. J. 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.
103. J. D. OHLIN, K. GOVERN, & C. FINKELSTEIN , CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS. (Oxford University Press 2015)
104. K. 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/.
105. R. 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/.
106. C. 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/.
107. Id.
108. C. LAUTERWASSER, OPPORTUNITIES AND RISKS OF NANOTECHNOLOGY (The OECD International Futures Programme n.d.).
109. G. ORWELL, 1984 (Harcourt Brace Publishers 1949).
110. A. HUXLEY, BRAVE NEW WORLD (Chatto and Windus Publishers 1931).
111. F. KAPLAN, DARK TERRITORY: THE SECRET HISTORY OF CYBER WAR (Simon & Schuster Publishers 2016).