International Journal of Social Science And Human Research

ISSN(print): 2644-0679, ISSN(online): 2644-0695

Volume 05 Issue 03 March 2022

DOI: 10.47191/ijsshr/v5-i3-45, Impact factor- 5.871

Page No: 1050-1073

In Light of The American Departure From Afghanistan, Does Network-Centric Warfare Adequately Prepare The United States to Address Future Cyber Activities by The Taliban?

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

ABSTRACT

The issue considered in this article is whether the United States is prepared adequately to address the cyber activities of the Taliban in the future in light of the recent American departure from Afghanistan. The first section defines and discusses cyber espionage, cyber sabotage, cyber terrorism, and cyber warfare. The following section outlines the notion of network-centric warfare and its relationship to the various cyber-attacks. The third section contains a brief history of the Taliban, cumulating in assessing the current political situation in Afghanistan. The paper's final section describes what adequate preparedness means for individuals, corporations, and the government. The paper concludes that the Taliban are not likely to be a cyber threat to the United States in the short term. However, as time progresses and the Taliban consolidates their political power, effectively defeating the Islamic State and insurgents in Panjshir, the United States will likely experience cyber attacks from the Taliban.

KEYWORDS: Afghanistan, Cyber Espionage, Cyber Sabotage, Cyber Terrorism, Cyberwar, Network-Centric Warfare, Taliban

The following abbreviations are used in this manuscript:

Abbreviation	Description
CIA	Central Intelligence Agency
FBI	Federal Bureau of Investigation
GID	Saudi Arabian General Intelligence Directorate
IoT	Internet of Things
ISI	Pakistani Inter-Service Intelligence Agency
NATO	North Atlantic Treaty Organization
NGO	Non-Government Organization
NSA	National Security Agency
UAE	United Arab Emirates
UN	United Nations
UNSC	United Nations Security Council

INTRODUCTION

On August 31, 2020, the United States departed Afghanistan. For the previous 20 years, the Taliban has been the focus of an intense military campaign by the United States, branding the entity as an insurgency organization.[1] There has been at least one attempt to have the Taliban classified as a terrorist group, but these efforts have failed so far.[2] Now that the United States has left Afghanistan and the Taliban are effectively in control of the government, the question begging to be answered is whether the Taliban poses a cyber threat to this country. If so, then is the United States adequately prepared to deal with yet another cyber threat? If not, at least in the short term, how long will it be before the Taliban become a cyber threat? And, more importantly, given the state of cyber preparedness in the United States, is America adequately prepared, or is additional preparation required?

[1] Lindsay Maizland, *The Taliban in Afghanistan*, THE COUNCIL OF FOREIGN RELATIONS (Sep. 15, 2021), available at https://www.cfr.org/backgrounder/taliban-afghanistan.

[2] Press Release, SEN. MARCO RUBIO, *Rubio Introduces Bill to Designate Taliban As a Foreign Terrorist Organization* (Sep. 15, 2021), https://www.rubio.senate.gov/public/index.cfm/2021/9/rubio-introduces-bill-to-designate-taliban-as-a-foreign-terrorist-organization.

These questions have no straightforward answers. Analyzing cyber espionage, sabotage, terrorism, and cyberwar is entirely appropriate. Furthermore, an appreciation of network-centric warfare with its myriad facets is in order. No analysis of the Taliban's threat would be complete without a brief organizational history. Finally, a discussion of adequate preparedness is essential to understand the threat presented by the Taliban. It is to these topics that this paper is addressed.

DEFINITIONS OF TERMS

This section contains a discussion of the definitions of cyber espionage, cyber sabotage, cyber terrorism, and cyberwar, respectively. The descriptions are general and not limited by the type of government, business, or organization subject to cyber activity. The final subsection explores the similarities and differences between the definitions.

DEFINITION OF CYBER ESPIONAGE

Cyber espionage involves employing computer networks to gain illegal access to secret or confidential information that is held by a government, a business, or some other organization.[3] Cyber espionage aims to steal classified data, sensitive data, or intellectual property to gain an economic or political advantage over a particular company or government.[4] Cyber espionage is the act of spying or employing spies to obtain information regarding the plans or activities of a corporation, government agency, or some other type of organization.[5]

In one sense, cyber espionage is much easier than traditional espionage.[6] Traditionally, it is difficult to recruit a spy, train the spy, and then put the spy in the target organization to copy or exfiltrate the desired information.[7] Also, with traditional espionage, there is always the possibility that the spy is gathering false information that has been purposefully planted or the spy has become a double agent.[8] The idea here is that the spy collects low-grade information that is of little value to the spying organization.[9] In contrast, the spy is usually not physically present in the target organization with cyber espionage. In most cases, the spy may be located hundreds, if not thousands, of miles away from the target organization while working from a remote computer, thereby making attribution challenging to achieve.[10]

Two critical issues when discussing espionage and cyber espionage are *jus ad bellum* and *jus in bello*.[11] Here, *jus ad bellum* is the right to wage war by a sovereign, while *jus in bello* is the international law that governs how warfare is conducted.[12] With a few exceptions, *jus ad bellum* and *jus in bello* do not govern gathering data via cyber operations, such as the disclosure of confidential documents by Edward Snowden, the cyber-attacks on Estonia, Georgia, and Ukraine, or the asymmetric measures discussed by Qiao and Wang.[13] [14] [15] Even the Tallinn Manual does not explicitly address cyber espionage and intellectual property theft because international law is not applicable.[16] In other words, cyber espionage has its roots in the law of espionage because, for most scholars, espionage and cyber espionage are legal, citing that the practice of espionage is ubiquitous among sovereigns and because it promotes stability.[17]

---

[3] MICHAEL N. SCHMITT (GEN. ED.), TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Cambridge University Press 2017).
[4] *Id.*
[5] *Id.*
[6] RICHARD A. CLARKE, & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT (HarperCollins Publishers 2010).
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] Patrick Clark, *The Hotel Hackers Are Hiding in the Remote Control Curtains*, BLOOMBERG BUSINESSWEEK (Jun. 26, 2019), *available at* https://www.bloomberg.com/news/features/2019-06-26/the-hotel-hackers-are-hiding-in-the-remote-control-curtains.
[11] JENS DAVID OHLIN, KEVIN GOVERN, & CLAIRE FINKELSTEIN, CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS (Oxford University Press 2015).
[12] UNITED STATES DEPARTMENT OF DEFENSE, LAW OF ARMED CONFLICT DESKBOOK (CreateSpace Independent Publishing Platform 16th ed. Aug. 17, 2018).
[13] Jens David Ohlin, Kevin Govern, & Claire Finkelstein, *supra*, note 11.
[14] Donald L. Buresh, *Russian Cyber-Attacks on Estonia, Georgia, and Ukraine Including Tactics, Techniques, Procedures, and Effects*, 1 JOURNAL OF ADVANCED FORENSIC SCIENCES 2, 15-26 (Aug. 2021), *available at* DOI: 10.14302/issn.2692-5915.jafs-21-3930.
[15] LIANG QIAO, & XIANGSUI WANG, UN-RESTRICTED WARFARE (Echo Point Books & Media 1999).
[16] Jens David Ohlin, Kevin Govern, & Claire Finkelstein, *supra*, note 11.
[17] *Id.*

DEFINITION OF CYBER SABOTAGE

According to Rid, sabotage is a deliberate attempt by an individual or group to weaken or disable an economic or military system.[18] Seemingly by definition, all sabotage is technical in nature, where social engineering may be employed.[19] This includes cyber sabotage.[20] Sabotage is sometimes designed to disable machines or production processes temporarily while avoiding damaging anything using violence.[21] If sabotage is violently conducted, the primary targets are things rather than human beings, even when the sabotage aims to alter benefit-cost decisions made by decision-makers.[22] Sabotage is an indirect form of attack, where the target of any political violence is the mind of the opponent's decision-makers.[23] The reason is that the point of political violence is geared to change the minds of the decision-makers by snatching as much political visibility as possible.[24]

When cyber-attacks are involved, it is easy to distinguish between violent and non-violent attacks.[25] The reason is that cyber-attacks rarely can damage hardware and mechanical or industrial processes.[26] For example, in the Shamoon attack of Saudi Arabia's oil company Aramco, the payload was designed to destroy data by overwriting the boot sector of a hard disk and the hard disk's partition tables.[27] The effect of the attack was that Aramco experienced significant operational impacts, including losing intellectual property and disrupting critical systems.[28] Another example is the malware Wiper, where the software systematically attempted to delete gigabytes of data while operating stealthily and deleting itself at the end of an attack.[29] Here, Kaspersky Labs observed that the malware did leave traces of its activities despite its attempts to destroy data and specific files.[30] The one limitation of Shamoon and Wiper was that both malware programs targeted large energy companies with massive quantities of data.[31] Although the business network was the victim of both attacks, the industrial control networks were unaffected. The oil was still being pumped out of the ground and into oil pipelines and tankers.[32]

When examining cyber sabotage, the three places where cyber sabotage can occur are the human-machine interface, the supervisory computer system, and remote telemetry units that monitor machinery and need to be directed or controlled by a supervisory application.[33] As systems become increasingly standardized, the increase in efficiency, connectivity, and visibility comes at the price of increased vulnerability.[34] On the other hand, industrial control systems may be safer because of increased oversight and red teaming with increased visibility.[35] A red team is a group of individuals that attempts to expose an organization's cyber weaknesses.[36] Another reason industrial control systems may be becoming safer is increased vendor security.[37] And the third reason is, strangely enough, increased obscurity due to the highly complex nature of industrial control systems.[38] The most successful

[18] THOMAS RID, CYBER WAR WILL NOT TAKE PLACE (Oxford University Press 2013).
[19] *Id.*
[20] *Id.*
[21] Michael A. Warren, (Nov. 2010) (unpublished Master of Science thesis, Ohio University), *available at* https://etd.ohiolink.edu/apexprod/rws_etd/send_file/send?accession=ohiou1289446353&disposition=inline.
[22] Thomas Rid, *supra*, note 18.
[23] Parliamentary Office Staff, *Assessing the Risk of Terrorist Attacks on Nuclear Facilities*, PARLIAMENTARY OFFICE OF SCIENCE AND TECHNOLOGY (Jul. 2004), *available at* https://www.parliament.uk/globalassets/documents/post/postpr222.pdf.
[24] *Id.*
[25] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, & Julia Spiegel, *The Law of Cyber Attack*, 100 CALIFORNIA LAW REVIEW 4, 817-85 (Aug. 2012), *available at* https://www.jstor.org/stable/23249823.
[26] Thomas Rid, *supra*, note 18.
[27] *Id.*
[28] *Id.*
[29] Catalin Cimpanu, *New Iranian Data Wiper Malware Hits Bapco, Bahrain's National Oil Company*, ZDNET (Jan. 09, 2020), *available at* https://www.zdnet.com/article/new-iranian-data-wiper-malware-hits-bapco-bahrains-national-oil-company/.
[30] Thomas Rid, *supra*, note 16.
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] NIST Staff, *Red Team*, COMPUTER SECURITY RESOURCE CENTER (n.d.), *available at* https://csrc.nist.gov/glossary/term/red_team.
[37] Thomas Rid, *supra*, note 18.
[38] *Id.*

saboteur is an insider.[39] The reason is that insiders usually possess the most significant amount of knowledge regarding how a system works.[40] This is true when speaking about both traditional sabotage and cyber sabotage.[41]

DEFINITION OF CYBER TERRORISM

Cyber terrorism uses computers for politically motivated purposes to disrupt or instigate fear in society.[42] [43] Examples include worms, viruses, phishing, and other malware attacking personal computer hardware and software.[44] Cyber terrorism can also be defined as employing the Internet to direct or threaten violent kinetic acts whose consequences are losing life or serious bodily harm to attain political or ideological ends via intimidation.[45] Cyber terrorism can be narrowly defined as acts by terrorist organizations against information systems to create alarm, panic, or the physical disruption of known processes.[46] The definition of cyber terrorism can also include cybercrime, but then it may become difficult to distinguish between cyberterrorism from cybercrime.[47]

Skilled hackers can initiate significant damage to government computer systems, national security programs, hospital information systems, corporate information systems, and even any devices employed by individuals and connected to the Internet.[48] The result is that cyber terrorism can ensure that countries, corporations, and communities experience a seemingly perpetual fear of a future cyber attack, thereby furthering the political or ideological goals of a cyber-terrorist organization.[49] The Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), the National Security Agency (NSA), and a plethora of corporations and non-government organizations (NGOs) have dedicated time and financial resources to mitigate, if not eliminate, cyber-attacks and cyber-terrorism.[50] There have been some major and minor acts of cyberterrorism, including the April 2007 Russian attack on Estonia, a country that borders Russia and the Baltic Sea.[51] One of the outcomes of the Estonian attack is the international creation of the Tallinn Manual 1.0 and 2.0, defining and describing the nature of cyber terrorism.[52]

DEFINITION OF CYBERWAR

Cyberwar is the employment of computer technology to interrupt ominously the ongoing activities of a state or organization, public or private, by purposefully and knowingly attacking information systems for strategic or tactical military purposes.[53] Cyberwar is a form of asymmetric warfare where militarily weaker nations can informationally attack their militarily stronger military counterparts.[54] Cyberwarfare consists of any virtual attack on an enemy's computer and information systems that is politically motivated.[55] The offense is conducted on the Internet to disable information systems or steal or alter classified computer data.[56]

---

[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] ROBERT W. TAYLOR, TORI J. CAETI, D. KALL LOPER, ERIC J. FRITSCH, & JOHN LIEDERBACH, DIGITAL CRIME AND DIGITAL TERRORISM (Pearson Education, Inc. 2006).
[43] Peter W. Singer, *The Cyber Terror Bogeyman*, BROOKINGS INSTITUTE (Nov. 01, 2012), *available at* https://www.brookings.edu/articles/the-cyber-terror-bogeyman/.
[44] *Id.*
[45] Marin Ivezic, *The World of Cyber-Physical Systems & Rising Cyber-Kinetic Risks*, MARIN IVEZIC (Mar. 31, 2015), *available at* https://cyberkinetic.com/cyber-kinetic-security/cyber-kinetic-risks/.
[46] HEDIEH NASHERI, ECONOMIC ESPIONAGE AND INDUSTRIAL SPYING (Cambridge University Press 2005).
[47] *Id.*
[48] Lee Rainie, Janna Anderson, & Jennifer Connolly, *Cyber Attacks Likely to Increase*, PEW RESEARCH CENTER (Oct. 29, 2014), *available at* https://www.pewresearch.org/internet/2014/10/29/cyber-attacks-likely-to-increase/.
[49] BRANDON VALERIANO, & RYAN C. MANESS, CYBER WAR VERSUS CYBER REALITIES: CYBER CONFLICT IN THE INTERNATIONAL SYSTEM (Oxford University Press 2015).
[50] *Foreign Cyber Threats to the United States*, HEARING BEFORE THE COMMITTEE ON ARMED SERVICES: UNITED STATES SENATE ONE HUNDRED FIFTEENTH CONGRESS FIRST SESSION (Jan. 05, 2017), *available at* https://www.govinfo.gov/content/pkg/CHRG-115shrg33940/html/CHRG-115shrg33940.htm.
[51] Donald L. Buresh, *A Critical Evaluation of the Estonian Cyber Incident*, 1 JOURNAL OF ADVANCED FORENSIC SCIENCES 2, 7-14 (Nov. 03, 2020), *available at* DOI 10.14302/issn.2692-5915.jafs-20-3601.
[52] Michael N. Schmitt, *supra*, note 3.
[53] RICHARD STIENNON, THERE WILL BE CYBERWAR: HOW TO MOVE TO NETWORK-CENTRIC WARFIGHTING SET THE STAGE FOR CYBERWAR (IT-Harvard Press 2015).
[54] *Id.*
[55] *Id.*
[56] Richard A. Clarke, & Robert K. Knake, *supra*, note 6.

Cyberwarfare can include cyber sabotage or cyber espionage.[57] Cyber sabotage can disrupt the normal operations of military and financial computer systems that deal with communication, fuel, power, and even transportation infrastructures.[58] On the other hand, computer espionage includes security breaches where illegal exploitation methods are employed to disable computer networks and computer hardware or software to attain classified or even confidential business records such as trade secrets for political or financial advantage.[59]

Although public perception envisions a computer hacker as a disenfranchised teenager who foolishly breaks into computer systems for pure pleasure, the reality is that computer hackers these days are typically well-funded individuals that can belong to organized crime syndicates or employees of government agencies.[60] [61] The government-employed hackers that created the Stuxnet virus are a case in point.[62]

ANALYSIS OF THE DEFINITIONS

There are several differences and similarities among the definitions above. First, cyber espionage is considered to be a precursor or even a part of cyber warfare.[63] Traditional espionage has existed since the dawn of history.[64] Cyber espionage puts a cyber twist on a long-established pursuit of states to gain economic, financial, or political advantage against competing countries.[65] Second, like conventional terrorism, cyber terrorism is a tactic to generate fear, panic, or interference with the workings of standard processes.[66] [67]

Cyber terrorism is a relatively new activity only because of the recent emergence and dominance of the Internet.[68] The terrorism issue is that fear and panic can be debilitating condition that prevents a government or another organization from behaving to optimize its benefits.[69] The goal of cyber terrorism is not necessarily to prevent a government or an organization from functioning.[70] Instead, the more common aim of cyber terrorism is to limit the choices of a government or organization in a manner whereby the government or organization is acting according to the wishes of the terrorist group instead of the way that the government or organization desires to perform.[71]

Cyberwar or cyber-warfare seems to be a catch-all term that encompasses cyber espionage, cyber sabotage, cyber terrorism, and other types of cyber operations.[72] Although cyberwar typically deals with countries and military enemies, the term can take on additional meaning when employed in criminal, corporate, and even individual settings.[73] The fundamental notion is that the asymmetry of a relationship can warrant the employment of cyberwar when both government and non-government actors are opposed to each other.[74] This evolution of meaning can lead to the description of novel situations, where, for example, the term "cyberwar" could be accurately applied when the antagonists are not nation-states but rather major corporations that are vying for

---

[57] Thomas Rid, *supra*, note 18.
[58] *Id.*
[59] *Id.*
[60] Matthew Weaver, *Teenage Hackers Motivated by Morality Not Money, Study Finds*, THE GUARDIAN (Apr. 21, 2017), *available at* https://www.theguardian.com/society/2017/apr/21/teenage-hackers-motivated-moral-crusade-money-cybercrime.
[61] SUSAN W. BRENNER, CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE (Praeger 2010).
[62] Jens David Ohlin, Kevin Govern, & Claire Finkelstein, *supra*, note 11.
[63] Darien Pun, *Rethinking Espionage in the Modern Era*, 18 CHICAGO JOURNAL OF INTERNATIONAL LAW. 1, 353-91 (Jul. 2017), *available at* https://chicagounbound.uchicago.edu/cjil/vol18/iss1/10/.
[64] Thomas Rid, *supra*, note 18.
[65] *Id.*
[66] Alex Schmid, *Terrorism - The Definitional Problem*, 36 CASE WESTERN RESERVE JOURNAL OF INTERNATIONAL LAW 2, 375-419 (2004), *available at* https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1400&context=jil.
[67] Matthew J. Littleton, INFORMATION AGE TERRORISM: TOWARD CYBERTERROR, (Dec. 1995) (unpublished Master of Science thesis, Naval Postgraduate School), *available at* https://fas.org/irp/threat/cyber/docs/npgs/terror.htm#TOC.
[68] FRED KAPLAN, DARK TERRITORY: THE SECRET HISTORY OF CYBER WAR (Simon & Schuster 2016).
[69] Thomas Rid, *supra*, note 18.
[70] Shamsuddin Abdul Jalil, *Countering Cyber Terrorism Effectively: Are We Ready To Rumble?*, SANS INSTITUTE (Jun. 2003), *available at* https://www.giac.org/paper/gsec/3108/countering-cyber terrorism-effectively-ready-rumble/105154#:~:text=The%20most%20common%20objective%20of,on%20particular%20targets%20%5B2%5D.
[71] *Id.*
[72] Jordan Robertson, *Is There Really a Cyberwar? Term Might Be Misused*, PHYS.ORG (May 05, 2010), *available at* https://phys.org/news/2010-05-cyberwar-term-misused.html.
[73] Chris Colvin, Daniel B. Garrie, & Siddartha Rao, *Cyber Warfare and the Corporate Environment*, 2 JOURNAL OF LAW & CYBER WARFARE 1, 1-24 (Spring 2013), *available at* https://www.jstor.org/stable/26441239.
[74] Paul Strassman, *Asymmetric Cyberwarfare Demands a New Information Assurance Approach*, ARMED FORCES COMMUNICATIONS AND ELECTRONICS ASSOCIATION (Jul. 01, 2013), *available at* https://www.afcea.org/content/asymmetric-cyberwarfare-demands-new-information-assurance-approach.

economic and financial advantage.[75] All is fair in economic warfare, commonly known as competitive behavior, a fact one should never forget.[76]

NETWORK-CENTRIC WARFARE

In this section, network-centric warfare is discussed in some detail. The history of network-centric warfare will be outlined, followed by a discussion of the principles and objectives of network-centric operations. Third, the paper assesses how vulnerable network-centric warfare is to a cyber-attack. Finally, several recommendations are specified, highlighting how network-centric warfare can be improved when appropriate.

HISTORY of Network-Centric Warfare

In 1996, Admiral William Owens premiered the notion of a "system of systems."[77] The work discussed a system of intelligent sensors, precision weapons, and command and control systems that assured a rapid target assessment using smart sensors, thereby promoting distributed weapons.[78] In 1997, the Navy described its vision of connecting everyone to a standard technology to flatten the hierarchy of command, enhance precision, and increase the speed of command.[79] Network-centric warfare as a standalone concept appeared in an article by Cebrowski and Garstka but was fleshed out with Alberts and Stein in *Network Centric Warfare: Developing and Leveraging Information Superiority*.[80] [81] The text expounded a new theory of using a case study analysis approach to help expand situation awareness, control inventory accurately, etc.[82]

In 2001, Alberts, Garstka, and Signori authored, *Understanding Information Age Warfare*, a seminal work on network-centric warfare.[83] In 2003, Alberts, Garstka, and Hayes speculated that the current military environment is far too complicated to understand by any individual or organization.[84] However, in a battlespace, technology permits the sharing of information so that those performing military missions can pull data from various sources to ensure the success of a mission.[85]

PRINCIPLES AND OBJECTIVES OF NETWORK-CENTRIC OPERATIONS

According to Alberts, the basic tenets of network-centric warfare include:[86]

- Tenet 1: A robustly networked force improves information sharing.
- Tenet 2: Information sharing and collaboration enhance the quality of information and shared situational awareness.
- Tenet 3: Shared situational awareness enables self-synchronization.
- Tenet 4: These, in turn, dramatically increase mission effectiveness.

These tenets remarkably increase the effectiveness of missions because it ensures that network-centric operations are consistent with Mission Control doctrine.[87] The idea is to help military personnel do what needs to be accomplished without traditional orders by

---

[75] Chris Colvin, Daniel B. Garrie, & Siddartha Rao, *supra*, note 73.
[76] FREDERICK A. HAYEK, LAW, LEGISLATION AND LIBERTY: A NEW STATEMENT OF THE LIBERAL PRINCIPLES OF JUSTICE AND POLITICAL ECONOMY (Routledge Classics 2012).
[77] William Owens, *The Emerging U.S. System of Systems*, INSTITUTE FOR NATIONAL STRATEGIC STUDIES, 63 (Feb. 1996), *available at* http://www.dtic.mil/get-tr-doc/pdf?AD=ADA394313.
[78] *Id.*
[79] Corporate Initiatives Group, *C4ISR Forward . . . A Vision of the Future*. SAN DIEGO, CALIFORNIA: NAVAL COMMAND (Jul. 1997), *available a*t https://www.dtic.mil/dtic/tr/fulltext/u2/a434155.pdf.
[80] Arthur K. Cebrowski, & John H. Garstka, *Network-Centric Warfare - Its Origin and Future*, UNITED STATES NAVAL INSTITUTE (Jan. 1998), *available at* https://www.usni.org/magazines/proceedings/1998/january/network-centric-warfare-its-origin-and-future.
[81] DAVID ALBERTS, JOHN GARSTKA, & FREDERICK STEIN, NETWORK CENTRIC WARFARE: DEVELOPING AND LEVERAGING INFORMATION SUPERIORITY (Department of Defense: Command and Control Research Program 2nd. ed. 2003), *available at* http://www.dodccrp.org/files/Alberts_NCW.pdf.
[82] *Id.*
[83] DAVID ALBERTS, JOHN GARSTKA, RICHARD HAYES, R., & DAVID A. SIGNORI, UNDERSTANDING INFORMATION AGE WARFARE *(*Department of Defense: Command and Control Research Program 2001), *available at* https://www.voltairenet.org/IMG/pdf/Understanding_Information_Age_Warfare-2.pdf.
[84] DAVID ALBERTS, JOHN GARSTKA, RICHARD HAYES, R., & DAVID A. SIGNORI, UNDERSTANDING INFORMATION AGE WARFARE *(*Department of Defense: Command and Control Research Program 2001), *available at* https://www.voltairenet.org/IMG/pdf/Understanding_Information_Age_Warfare-2.pdf.
[85] *Id.*
[86] DAVID S. ALBERTS, INFORMATION AGE TRANSFORMATION: GETTING TO A 21ST CENTURY MILITARY (Department of Defense: Command and Control Research Program 2002), *available at* http://dodccrp.org/files/Alberts_IAT.pdf.
[87] *Id.*

providing individuals with an increased understanding of the command's intent, thereby ensuring considerable freedom of action by combat troops.[88] [89] By exploiting the collective knowledge of a battlefield, the fog and friction of war can be dramatically reduced.[90]

VULNERABILITY OF NETWORK-CENTRIC WARFARE TO A CYBER-ATTACK

A chain is only as strong as its weakest link. The weakest link in network-centric operations and warfare is the communication between those on the edge of the battlespace and the supporting personnel and systems.[91] Communications can be hacked. A soldier's information request on the front can be rerouted using the *man-in-the-middle* hack.[92] Here, a request for information from a soldier can be siphoned off and then altered in clever and devious ways so that the recipient behind the field of battle receives false information that the hacker has changed.[93] In another "man-in-the-middle" scenario, the data from individuals on the edge is correctly sent, but the "man-in-the-middle" hack occurs when the information requested is sent back to the field soldier.[94] In this case, the hacker alters the information requested. In the previous point, the request itself was altered.[95] A third possibility is that the hacker changes both the request and the information requested without knowing the field solder or the supporting personnel.[96] In this case, the data is hacked coming and going.

One way to circumvent this problem is to employ asymmetric encryption when sending and receiving data.[97] With asymmetric encryption, there is a public key and a private key.[98] However, suppose a machine that uses asymmetric encryption is captured, and in battle, there is a high likelihood that this will occur. In that case, the adversary could gain access to both the public and private keys.[99] Like the enigma machine that Germans used in World War II, there has to be a mechanism that changes the keys periodically[100]. For asymmetric keys, the public key and the private key are related to each other, meaning that if the user needs to change a private key, then the associated public key must also change.[101]

One vulnerability in network-centric warfare occurs when the amount of information being transmitted and received exceeds the bandwidth of the communication channel.[102] This can happen due to a denial-of-service attack, where the bandwidth is insufficiently robust.[103] The result is that typically no requests are transmitted from the individuals on the edge to the supporting personnel behind the lines of conflict.[104] According to Wilson, command could disconnect from some individuals, leaving them to

---

[88] *Id.*

[89] MARIUS VASSILIOU, DAVID S. ALBERTS, & JONATHAN R. AGRE, C2 RE-ENVISIONED: THE FUTURE OF THE ENTERPRISE (Chemical Rubber Company Press 2015).

[90] Clay Wilson, *Network Centric Operations: Background and Oversight Issues for Congress*, CONGRESSIONAL RESEARCH SERVICE (Mar. 15, 2007), *available at* https://www.researchgate.net/publication/235121618_Network_Centric_Operations_Background_and_Oversight_Issues_for_Congress.

[91] MICHAEL E. WHITMAN, & HERBERT J. MATTORD, PRINCIPLES OF INFORMATION SECURITY (Cengage Learning 2016).

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] Gustavus J. Simmons, *Symmetric and Asymmetric Encryption*, 11 ACM COMPUTING SURVEYS 4, 305-30 (Dec. 1979), *available at* https://doi.org/10.1145/356789.356793.

[98] *Id.*

[99] RYAN RUSSELL, TIMOTHY MULLEN, & JOHNNY LONG, STEALING THE NETWORK: THE COMPLETE SERIES COLLECTOR'S EDITION (Elsevier Publishing 2009), *available at* https://books.google.com/books?id=4csyeZaEP4cC&pg=PA651&lpg=PA651&dq=stealing+a+computer+that+uses+asymmetric+encryption&source=bl&ots=tJLyiwwBiI&sig=ACfU3U1y2COvwBkp5fsPZwhdcuYDacPSww&hl=en&sa=X&ved=2ahUKEwjbzs2kwrbyAhWKbs0KHXU3Ck4Q6AF6BAg5EAM#v=onepage&q=stealing%20a%20computer%20that%20uses%20asymmetric%20encryption&f=false.

[100] DAVID MOWRY, GERMAN CIPHER MACHINES OF WORLD WAR II (National Security Agency: Center for Cryptologic History rev. ed. 20014), available at https://www.nsa.gov/Portals/70/documents/about/cryptologic-heritage/historical-figures-publications/publications/wwii/german_cipher.pdf.

[101] Gustavus J. Simmons, *supra*, note 97.

[102] Henry Kamradt, & Douglas MacDonald, *The Implications of Network-Centric Warfare for United States and Multinational Military Operations*, UNITED STATES NAVAL WAR COLLEGE (Dec. 31, 1998), *available at* https://apps.dtic.mil/sti/pdfs/ADA430553.pdf.

[103] *Id.*

[104] *Id.*

fend for themselves to maintain the more essential connections.[105] This may be unreasonable because the attacker could always increase the intensity of the attack once it is discovered that the transmission volume has decreased.[106] The other problem with this situation is that the disconnected individuals may be poorly trained to handle the issue independently.[107] It is well known that people become accustomed to support, just like an inmate who becomes dependent on being institutionalized.[108] Without support from command, the individuals in the field will likely surrender just because they are having difficulty thinking for themselves.[109]

A third vulnerability can occur when the enemy uses the terrain to disguise their presence on the battlefield, so network-centric operations cannot detect them.[110] This can sometimes be achieved by an adversary that employs low-tech responses to high-tech weapons, tactics, and strategy.[111] Many times, low-tech weapons, tactics, and strategy are something to be reckoned with. The problem with high-tech solutions is that individuals can become altogether too dependent on their devices.[112] For example, when the author has traveled to downtown Chicago, using the L-train, almost all of the people waiting on the platform for the train to arrive, or in the train itself, were glued to their cell phones. The open question is, what would these people do without their cell phones? Could they cope in the world without cell phones? Probably not.

The final vulnerability of network-centric warfare under discussion herein can occur when military or civilian leadership simply circumvents or overrides the freedom of choice available to combat troops under network-centric warfare tenets.[113] [114] [115] Suppose combat troops are specifically ordered not to employ their initiative and not exploit network-centric principles in an operational setting. In that case, the advantages promoted by network-centric warfare may fail.[116] [117] [118] For example, in August 2020, President Biden withdrew military personnel from Afghanistan before evacuating the American civilian population and the Afghan personnel who worked with Americans during the 20 years that the United States was in Afghanistan.[119] [120] The result was complete chaos.[121] It is unclear how many Americans were living in Afghanistan at the time.[122] It could have been as low as 10,000 individuals or as high as 40,000 people.[123] The number of Afghans who worked with America or were part of the Afghan Army \was tens of thousands of people.[124]

---

[105] Clay Wilson, *supra*, note 90.
[106] *Id*.
[107] *Id*.
[108] KIMBERLY S. YOUNG, & CRISTIANO NABUCO, DE ABREU (EDS.), INTERNET ADDICTION: A HANDBOOK AND GUIDE TO EVALUATION AND TREATMENT (John Wiley & Sons, Inc. 2011), *available at* http://www.ssu.ac.ir/cms/fileadmin/user_upload/Moavenatha/MBehdashti/ravan/pdf/faaliyatha/pptfiles/INTERNET_ADDICTION.pdf#page=39
[109] *Id*.
[110] Henry Kamradt, & Douglas MacDonald, *supra*, note 102.
[111] *Id*.
[112] *Id*.
[113] Joseph H. Scherrer, *Risks and Vulnerabilities of Network-Centric Forces: Insights from the Science of Complexity*, NAVAL WAR COLLEGE (Feb. 03, 2003), *available at* https://apps.dtic.mil/sti/citations/ADA415474.
[114] Clay Wilson, *supra*, note 90.
[115] David L. Peeler, Jr., & Michael P. Dahlstrom, *Network Centric Warfare: Advantages and Disadvantages*, STRATEGIC IMPACT NO. 3 (2003), *available at* https://www.proquest.com/openview/364a2a648a2241267b93979755e55788/1?pq-origsite=gscholar&cbl=1876337.
[116] Joseph H. Scherrer, *supra*, note 113.
[117] Clay Wilson, *supra*, note 90.
[118] David L. Peeler, Jr., & Michael P. Dahlstrom, *supra*, note 115.
[119] Terri Moon Cronk, *Biden Announces Full U.S. Troop Withdrawal from Afghanistan by Sept. 11*, UNITED STATES DEPARTMENT OF DEFENSE (Apr. 14, 2021), *available at* https://www.defense.gov/Explore/News/Article/Article/2573268/biden-announces-full-us-troop-withdrawal-from-afghanistan-by-sept-11/.
[120] Madeleine Ngo, *Biden Defends Decision to Pull Out of Afghanistan*, THE NEW YORK TIMES (Aug. 18, 2021), *available at* https://www.nytimes.com/live/2021/08/16/us/politics-news.
[121] Paul D. Shrinkman, *Chaos, Violence at Kabul Airport as U.S. Tries to Complete Afghanistan Evacuation*, U.S. NEWS & WORLD REPORT (Aug. 16, 2021), *available at* https://www.usnews.com/news/world-report/articles/2021-08-16/chaos-violence-at-kabul-airport-as-us-tries-to-complete-afghanistan-evacuation.
[122] Juliegrace Brufke, *Biden team vague on evacuating Americans, allies from Afghanistan after Aug. 31*, THE NEW YORK POST (Aug. 17, 2021), *available at* https://nypost.com/2021/08/17/biden-team-vague-on-evacuating-americans-allies-from-afghanistan/.
[123] Mark Moore, *David Petraeus calls Afghanistan a 'Dunkirk Moment'*, THE NEW YORK POST (Aug. 17, 2021), *available at* https://nypost.com/2021/08/17/david-petraeus-calls-afghanistan-a-dunkirk-moment/.
[124] Miriam Jordan, *Thousands Who Helped the U.S. in Afghanistan Are Trapped. What Happens Next?*, THE NEW YORK TIMES (Aug. 16, 2021), *available at* https://www.nytimes.com/2021/08/16/us/afghanistan-visa-refugees-us.html.

In contrast, the British sent 900 paratroopers into Kabul to extract approximately 4,000 British subjects from Afghanistan.[125] For the British soldiers to successfully remove British subjects from Afghanistan, these soldiers practiced significant freedom of action to achieve an objective under the chaotic conditions that were present in Kabul as espoused in Tenet 4 of network-centric warfare.[126] French soldiers were also actively locating and evacuating French citizens from Kabul,[127] while although initially stumbling, Germany sent helicopters to rescue Afghan support staff.[128] Finally, the Canadian government considered using special forces to retrieve Afghan interpreters and support staff from Kabul.[129] Thus, it is apparent that when the tenets of network-centric warfare are followed, as exemplified by NATO members other than the United States, and are not circumvented for political reasons by senior military and civilian leaders, network-centric principles and operations are remarkably successful because individual soldiers possess sufficient autonomy to make independently effective decisions.[130] [131]

Based on the discussion above, it is apparent that the United States military should not become too dependent on technology with the understanding that it is easier said than done. Also, when network-centric tenets are adhered to, the results are remarkably positive. The reason is that network-centric warfare is perceived as a mechanism to reduce the fog and friction of war with the omnipresent agenda of reducing cost.[132] In terms of economics, the issue is essentially a capital-labor decision.[133] Network-centric warfare substitutes the capital of technology for the labor of traditional soldiering with the hope that a capital-intensive solution will reduce battlefield costs.[134] In essence, by focusing on network-centric warfare, the United States military attempts to obtain the biggest bang per dollar spent, no pun intended.[135]

According to Keynesian economics, although the reduction in costs will probably occur over the long run, it is the most critical short-run cost.[136] The implication is that the long-run will take care of itself, and only the short-run that matters.[137] It is suggested that the United States military spend a fraction of money ensuring that soldiers can perform efficiently and effectively with and without technology. The reason is that it is vital to take advantage of technology while at the same time ensuring that a mission is not compromised when the technology is lacking.

A BRIEF HISTORY OF THE TALIBAN

In this section, a brief history of the Taliban `will be discussed. The topics include the origin of the Taliban, the Soviet intervention in Afghanistan, the Afghan civil war, the First Islamic Emirate of Afghanistan, the attack on September 11, 2001, and the days following, the American invasion in 2001, the American occupation from 2001 to 2021, the American departure from Afghanistan, and the Second Islamic Emirate of Afghanistan. Each topic will be discussed in turn.

---

[125] Robert Clark, *As NATO Allies Flounder, British Troops Are Leading by Example at Kabul Airport*, THE TELEGRAPH (Aug. 18, 2021), *available at* https://www.telegraph.co.uk/news/2021/08/19/nato-allies-flounder-british-troops-leading-example-kabul-airport/.

[126] *Id.*

[127] James R. Webb, *As US Military Sticks to Airport, British and French Forces Are Rescuing their Citizens in Kabul: Reports*, MILITARY TIMES (Aug. 19, 2021), *available at* https://www.militarytimes.com/flashpoints/afghanistan/2021/08/19/as-us-military-sticks-to-airport-british-and-french-forces-are-rescuing-their-citizens-in-kabul-reports/.

[128] Loveday Morris, *Amid Sharp Criticism, Germany Stumbles in Late Efforts to Rescue Afghan Support Staff*, THE WASHINGTON POST (Aug. 22, 2021), *available at* https://www.washingtonpost.com/world/germany-afghans-evacuation/2021/08/21/d33941ce-0202-11ec-ba7e-2cf966e88e93_story.html.

[129] Robert Fife, *Canadian special forces may be used to rescue Afghan interpreters, support staff from Kabul: Sajjan*, THE GLOBE AND MAIL (Aug. 22, 2021), *available at* https://www.theglobeandmail.com/politics/article-canadian-special-forces-may-be-used-to-rescue-afghan-interpreters/.

[130] Victor Davis Hanson, *Victor Davis Hanson: If Biden were a Republican, Dems in Congress would have impeached him. They should*, FOX NEWS (Aug. 22, 2021), *available at* https://www.foxnews.com/opinion/biden-republican-democrats-congress-impeached-victor-davis-hanson.

[131] Ryan Morgan, *US Has No Plans to Rescue Americans, Afghans Stranded behind Taliban Lines Outside Kabul A, Airport*, AMERICAN MILITARY NEWS (Aug. 18, 2021), *available at* https://americanmilitarynews.com/2021/08/us-has-no-plans-to-rescue-americans-afghans-stranded-behind-taliban-lines-outside-kabul-airport/.

[132] CHRISTOPHER R SMITH, NETWORK CENTRIC WARFARE, COMMAND, AND THE NATURE OF WAR (Land Warfare Studies Centre (Australia) 2010), *available at* https://researchcentre.army.gov.au/sites/default/files/sp318ncwcommandandnatureofwarchristopher_smith.pdf.

[133] PAUL KRUGMAN, & ROBIN WELLS, ECONOMICS (Worth Publishers 5th ed. 2017).

[134] Paul Murdock, *Principles of War on the Network-Centric Battlefield: Mass and Economy of Force*, 32 THE US ARMY WAR COLLEGE QUARTERLY: PARAMETERS 1 (Spring 2002), *available at* https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2082&context=parameters.

[135] Paul Krugman, & Robin Wells, *supra*, note 133.

[136] JOHN MAYNARD KEYNES, THE GENERAL THEORY OF EMPLOYMENT, INTEREST, AND MONEY (Palgrave Macmillan 1936).

[137] *Id.*

ORIGIN OF THE TALIBAN (THE 1970S)

According to Jain, although the Taliban emerged as a political force in Afghanistan in the 1990s, to understand the group's history, one must go back to the Saur Revolution of 1978.[138] By the 1970s, Afghanistan had been becoming a modern state for years.[139] Both the United States and the Soviet Union were keenly involved in modernizing Afghanistan's infrastructure and extending their power over Central and South Asia. These actions resulted in a flood of foreign aid, where the primary employer in Afghanistan became the Afghan government, thereby leading to systemic corruption and an eventual revolution.[140]

In the late 1970s, different ideologies struggled for dominance. Marxists consisted of young activists, journalists, professors, and military commanders on one side.[141] On the other side were the Muslims that desired a Muslim Brotherhood-like Islamic state.[142] Daud Khan was then the president of Afghanistan, and he initially aligned himself with the young military commanders. However, given the real threat of a revolutionary coup, Khan began quashing opposing groups. In April 1978, Khan was deposed by a coup, resulting in a Marxist-Leninist People's Republic of Afghanistan.[143] After purging the Communist party, the new Afghan government began suppressing Islamists and other groups opposed to the government. When the inevitable resistance occurred, the United States channeled money to Pakistan's intelligence services allied with the Afghan Islamists.[144]

The United States joined with the mujahedeen, a loose coalition of resistance groups. There were also leftist groups that the Afghan communists purged. All of these groups were opposed to the authoritarian communist government.[145] When Afghan leader Nur Mohammad Taraki was assassinated in 1979 by his second-in-command, Hafizullah Amin, the Soviets were afraid that the United States would exploit the increased instability in Afghanistan. The Soviets decided to invade Afghanistan and thus ensured that the United States would channel even more money to the mujahedeen.[146]

SOVIET INTERVENTION IN AFGHANISTAN (1978 – 1992)

On December 24, 1979, the Soviet Union invaded Afghanistan to sustain the Soviet-Afghan Friendship Treaty of 1978.[147] On December 27, Babrak Karmal, the exiled leader of the Parcham faction of the Marxist People's Democratic Party of Afghanistan (PDPA), was installed by the Soviets as Afghanistan's new head of government.[148] After the Soviet invasion and occupation of Afghanistan in 1979, the mujahideen engaged in a fierce war with the Soviet military.[149] In the meantime, Pakistan's President Muhammad Zia-ul-Haq was afraid that the Soviets would also invade Balochistan, Pakistan. Ziz-ul-Haq sent Akhtar Abdur Rahman to Saudi Arabia to gather Islamic support for the Afghan resistance against the Soviet forces. The United States Central Intelligence Agency (CIA) and Saudi Arabian General Intelligence Directorate (GID) gave equipment through the Pakistani Inter-Service Intelligence Agency (ISI) to the Afghan mujahideen.[150]

When the Soviets ventured out of their bases into the countryside to combat the mujahideen, they faced fierce resistance by fighters who would attack and then fade into the Afghan mountains.[151] The mujahideen viewed the Soviets as Christians or atheists defiling Islam and their culture, thereby engaging in a jihad or holy war against the Soviets. In 1987, the United States gave the mujahideen shoulder-held Stinger missiles, which the Afghan resistance used to shoot down Soviet aircraft.[152] With victory being unfeasible, the new Soviet leader and General Secretary of the Russian Communist Party, Mikhail Gorbachev, decided to get out of Afghanistan. The last Soviet soldier left the country on February 15, 1989.[153]

---

[138] Kalpana Jain, *The History of the Taliban Is Crucial in Understanding Their Success Now – And Also What Might Happen Next*, THE CONVERSATION (Aug. 26, 2021), *available at* https://theconversation.com/the-history-of-the-taliban-is-crucial-in-understanding-their-success-now-and-also-what-might-happen-next-166630.
[139] *Id.*
[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] *Id.*
[144] *Id.*
[145] *Id.*
[146] *Id.*
[147] History.com Editors, *Soviet Union InvadesAfghanistan*, HISTORY.COM (Nov. 24, 2009), *available at* https://www.history.com/this-day-in-history/soviet-tanks-roll-into-afghanistan.
[148] *Id.*
[149] Kalpana Jain, *supra*, note 138.
[150] Colin Price, Pakistan: *A Plethora of Problems*, 3 GLOBAL SECURITY STUDIES 1, 53-62 (Winter 2012), *available at* https://www.semanticscholar.org/paper/Pakistan%3A-A-Plethora-of-Problems-Price/b7c99634746e77be1bfb50346198b5d4779214f5.
[151] History.com Editors, *supra*, note 147.
[152] *Id.*
[153] *Id.*

AFGHAN CIVIL WAR (1992 – 1996)

After the departure of the Soviets and the fall of the Soviet-backed government, in April 1992, the Afghan political parties backed the Peshawar Accord that created the Islamic State of Afghanistan and appointed an interim government.[154] However, because rival political factions were vying for total power over Afghanistan, the government was crippled from its inception because several Afghan political parties refused to participate in the interim government. In particular, Hekmatyar's Hezb-e Islami Gulbuddin party would not recognize the interim government. However, in April 1992, Hekmatyar infiltrated Kabul and took control of the government.[155] Hekmatyar obtained operational, financial, and military support from Pakistan's Inter-Services Intelligence (ISI),[156] while Iran assisted Hezbe Wahdat, and Saudi Arabia sustained the Ittihad-i Islami faction.[157] The struggle between these political factions resulted in the Afghan civil war.

Because of how quickly the civil war started, many government agencies for the Islamic State of Afghanistan were not formed. Although individuals committed atrocities within each faction, ceasefires negotiated by the interim government fell apart within days.[158] In contrast, there was little to no fighting in the northern areas in Afghanistan that Ahmad Shah Massoud controlled. Southern Afghanistan was controlled by local leaders such as Gul Agha Sherazi and their militias.

FIRST ISLAMIC EMIRATE OF AFGHANISTAN (1996 – 2001)

In 1995, the Taliban expanded from their base of operations in Kandahar, expanding over a sizeable territorial area. In early 1995, the Taliban moved towards Kabul but were repelled by government forces. After several setbacks, the Taliban successfully took control of Herat on September 5, 1995. On September 26, 1995, the Taliban prepared for a major offensive and entered Kabul on September 27, 1996, establishing the First Islamic Emirate of Afghanistan.[159]

The goal of the Taliban was to create an Islamic state through adherence to Sharia law, where the Hanafi school of Islamic jurisprudence dominated the whole country of Afghanistan. By 1998, approximately 90 percent of Afghanistan was controlled by the Emirate.[160] However, because seemingly continuous warfare raged through the country for 20 years, Afghanistan's infrastructure and economy were in shambles. The was no running water, very little electricity, an insufficient number of telephones, or functioning roads. Energy supplies were scarce. The clan and family structure also withered, where 25 percent of children died before their fifth birthday.[161] The Taliban leaders mistrusted Western NGOs that desired to help the civilian population, so aid was spotty. When the heads of three United Nations (UN) agencies protested that a female attorney from the UN High Commissioner for Refugees was required to speak behind a curtain so that Taliban leaders would not see her face, they were expelled.[162] When the UN added female Muslim staffers, the Taliban required a *mahram* or a blood relative to accompany them.[163] In July 1998, the Taliban closed all NGO offices in Kabul by force after the NGOs refused to move to the bombed-out Polytechnic College as they were ordered. The building had neither electricity nor running water.[164] As the price of food increased and conditions generally deteriorated, Planning Minister Qari Din Mohammed stated that "God the Almighty will feed everyone one way or another" and that the NGOs were leaving Afghanistan of their own choice.[165]

---

[154] John Sifton, *Blood-Stained Hands: Past Atrocities in Kabul and Afghanistan's Legacy of Impunity*, HUMAN RIGHTS WATCH (Jul. 6, 2005), *available at* https://www.hrw.org/report/2005/07/06/blood-stained-hands/past-atrocities-kabul-and-afghanistans-legacy-impunity#.

[155] *Id.*

[156] NEAMATOLLAH NOJUMI. THE RISE OF THE TALIBAN IN AFGHANISTAN: MASS MOBILIZATION, CIVIL WAR, AND THE FUTURE OF THE REGION (Palgrave 1st ed. 2002 1st ed.).

[157] AMIN SAIKAL, MODERN AFGHANISTAN: A HISTORY OF STRUGGLE AND SURVIVAL (I.B. Tauris & Co.1st ed. 2006).

[158] John Sifton, *Blood-Stained Hands: Past Atrocities in Kabul and Afghanistan's Legacy of Impunity*, HUMAN RIGHTS WATCH (Jul. 6, 2005), *available at* https://www.hrw.org/report/2005/07/06/blood-stained-hands/past-atrocities-kabul-and-afghanistans-legacy-impunity.

[159] AMIN SAIKAL, MODERN AFGHANISTAN: A HISTORY OF STRUGGLE AND SURVIVAL (I. B. Tauris & Co. 2006).

[160] Lindsay Maizland, *The Taliban in Afghanistan*, COUNCIL ON FOREIGN RELATIONS (Sep. 15, 2021), *available at* https://www.cfr.org/backgrounder/taliban-afghanistan.

[161] Robert Nichols, *Afghan Historiography: Classical Study, Conventional Narrative, National Polemic*, 3 HISTORY COMPASS 1 (Dec 21, 2005), *available at* https://doi.org/10.1111/j.1478-0542.2005.00141.x.

[162] AHMED RASHID, AHMED (2000), TALIBAN: MILITANT ISLAM, OIL AND FUNDAMENTALISM IN CENTRAL ASIA 65 (Yale University Press 2000).

[163] *Id.* at 71.

[164] ReliefWeb Staff, *MSF and Other Aid Organizations Evicted from Kabul*, RELIEFWEB (Jul. 21, 2998), *available at* https://reliefweb.int/report/afghanistan/msf-and-other-aid-organizations-evicted-kabul.

[165] Katherine Haddon, *Afghanistan Marks 10 Years Since War Started*, YAHOO! NEWS (Oct. 6, 2011), *available at* https://web.archive.org/web/20111010055026/http://news.yahoo.com/afghanistan-marks-10-years-since-war-started-211711851.html.

Overall, starting in 1994, the Taliban was financially supported by the Pakistani ISI.[166] According to Rashid, from 1994 to 1999, about 80,000 to 100,000 Pakistani trained and fought for the Taliban.[167] In 2000, the United Nations Security Council (UNSC) established an arms embargo against military support to the Taliban.[168] In 2001, about 30,000 Pakistani nationals fought for the Taliban.[169]

In 1996, in response to the Taliban, Ahmad Shah Massoud and Abdul Rashid Dostum, two former enemies, created the United Front, or the Northern Alliance. In 1998, after the battle for the northern city of Mazar-i-Sharif, Dostum was defeated and went into exile. Under Massoud, democratic institutions were created where women and girls were not forced to wear burqas and were permitted to work and attend school. The Taliban repeatedly offered Massoud to join them by enticing him to become the prime minister of Afghanistan. However, Massoud refused the offer, stating that he was fundamentally against the Afghan Emirate system.[170] In early 2001, Massoud and several Afghan leaders addressed the European Parliament, stating without the support from the Pakistani government and Osama Bin Laden, the Taliban were fundamentally a weak military and political force. On September 9, 2001, two days before the 9/11 attack on the World Trade Center in New York City, Massoud died in a helicopter, taking him to a hospital. Hundreds of thousands of his people attended his funeral.[171]

ATTACK ON SEPTEMBER 11, 2001, AND THE DAYS FOLLOWING

On September 11, 2001, the World Trade Center in New York City and the Pentagon in Washington, DC were attacked. There was also a highjacked airplane that crashed in Pennsylvania.[172] On September 20, 2001, President George W. Bush spoke in a joint session of Congress, blaming Al-Qaeda for the attack and that the Taliban supported the Al-Qaeda leadership. In the speech, Bush demanded that the Taliban (1) deliver all Al-Qaeda leaders to the United States, (2) release all unjustly imprisoned foreign nationals, (3) protect foreign journalists, diplomats, and aid workers, (4) close terrorist training camps, (5) hand over terrorists, and (6) allow the United States to inspect terrorist training camps.[173] The United States asked the international community to support a military effort to overthrow the Taliban. The UNSC was unwilling to authorize a military venture into Afghanistan, but the North Atlantic Treaty Organization (NATO) approved the campaign against Afghanistan as a self-defense response.[174] The Taliban ambassador to Pakistan responded by asking the United States for evidence that Osama Bin Laden was responsible for the attack and that Bin Laden be tried in an Afghan court.[175] There was no apparent compromise possible.

AMERICAN INVASION OF AFGHANISTAN (2001)

On October 7, 2001, the United States, with the help of the United Kingdom, Canada, and other countries, some of which were NATO members, began military action against the Taliban and Al-Qaeda.[176] The intent behind the campaign was to overthrow the Taliban and ensure that Afghanistan was not used as a base for terrorism.[177] On October 14, 2001, the Taliban proposed that discussions be held where bin Laden would be handed over to a neutral country in exchange for halting the bombing, presuming

---

[166] JEANNE K. GIRALDO, & HAROLD A. TRINKUNAS, TERRORISM FINANCING AND STATE RESPONSES : A COMPARATIVE PERSPECTIVE 96 (Stanford University Press 2007).
[167] Ahmed Rashid, *supra*, note 162.
[168] DANIEL BYMAN, DEADLY CONNECTIONS: STATES THAT SPONSOR TERRORISM 195 (Cambridge University Press 2005).
[169] EDWARD GIRARDET. KILLING THE CRANES: A REPORTER'S JOURNEY THROUGH THREE DECADES OF WAR IN AFGHANISTAN 416 (Chelsea Green Publishing. 2011).
[170] Piotr Balcerowicz, *The Last Interview with Ahmad Shah Masood*, HOJA BAHAUDDIN (early August 2001), *available at* https://web.archive.org/web/20060925043421/http://www.orient.uw.edu.pl/balcerowicz/texts/Ahmad_Shah_Masood_en.htm.
[171] John F. Burns, *Threats And Responses: Assassination; Afghans, Too, Mark a Day of Disaster: A Hero Was Lost*, THE NEW YORK TIMES (Sep. 9, 2002), *available at* https://www.nytimes.com/2002/09/09/world/threats-responses-assassination-afghans-too-mark-day-disaster-hero-was-lost.html.
[172] Peter L. Bergen, *September 11 Attacks*, ENCYCLOPEDIA BRITANNICA (n.d.), *available at* https://www.britannica.com/event/September-11-attacks.
[173] George W. Bush, *Text: President Bush Addresses the Nation*, THE WASHINGTON POST (Sep.20, 2001) *available at* https://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bushaddress_092001.html.
[174] Press Release, NORTH ATLANTIC TREATY ORGANIZATION, *Statement by the North Atlantic Council* (Sep. 12, 2001), https://www.nato.int/docu/pr/2001/p01-124e.htm.
[175] John F. Burns, *A Nation Challenged: Last Chance; Taliban Refuse Quick Decision Over bin Laden*, THE NEW YORK TIMES (Sep. 18, 2001), *available at* https://www.nytimes.com/2001/09/18/world/a-nation-challenged-last-chance-taliban-refuse-quick-decision-over-bin-laden.html.
[176] CNN Staff, *Afghanistan Wakes After Night of Intense Bombings*, CABLE NEWS NETWORK (CNN) (Oct. 7, 2001), *available at* http://edition.cnn.com/2001/US/10/07/gen.america.under.attack/.
[177] George W. Bush, *Presidential Statement: Bush Announces Military Action Against Terrorist Infrastructure in Afghanistan*, CQ ALMANAC (Oct. 7, 2001), *available at* https://library.cqpress.com/cqalmanac/document.php?id=cqal01-106-6369-328096.

that the United States would provide evidence to the Taliban that bin Laden was involved with the attack of the United States.[178] The United States rejected this offer.

On November 9, 2001, Mazar-i-Sharif fell to the NATO coalition and the Northern Alliance with little resistance. In November 2001, and before the capture of Kunduz, the Pakistanis airlifted ISI military agents, military personnel, and other Taliban sympathizers out of Kunduz by the Pakistan Army to Pakistani airbases.[179] On the night of November 12, 2001, the Taliban abandoned Kabul, the capital of Afghanistan. On November 13, 2001, the Taliban also retreated from Jalalabad, and on November 15, 2001, the Taliban released eight Western aid workers. In December 2001, the Taliban relinquished Kandahar, their remaining stronghold, dispersing into the countryside.[180]

AMERICAN OCCUPATION OF AFGHANISTAN (2001 – 2021)

The United States military occupied Afghanistan for approximately 20 years. At first, Pashtun tribal chief, Hamid Karzai, was elected as the country's interim leader.[181] In December 2001, the Taliban were not invited to the Bonn Agreement because the United States did not want the Taliban to participate in the proceedings due to the Taliban's continued resurgence.[182] In 2003, the Taliban showed signs of a comeback and a restoration of an insurgence, proclaiming that they were prepared to conduct a guerrilla war against the United States.[183] On May 29, 2006, an American military truck in a convey lost control, killing one and injuring six people, resulting in a riot, where 20 people died, and 160 were injured.[184] The riot may have been caused by growing discontent with foreigners occupying Afghanistan.

In September 2007, then-President Karzai offered to conduct peace talks with the Taliban, but the United States resisted this effort, and the Taliban rejected the offer, citing the presence of foreign troops in the country.[185] By 2009, the Taliban had created a strong insurgency movement, known as Operation Al Faath, or *victory* from the Koran in the form of guerilla warfare. In December 2009, the Taliban offered to give the United States legal guarantees that Afghanistan would not be used to attack other countries. The United States did not respond.[186] In July 2016, it was reported that between 20 percent to 26 percent of Afghanistan was under the control of the Taliban.[187] [188] In August 2017, after the Taliban had killed 50 people in Kabul and President Trump stated that he wanted to win but also withdraw, the Taliban proclaimed that they would continue fighting to remove the foreign presence in their country.[189] On February 27, 2018, Afghan President Ashraf Ghani proposed unconditional peace talks with the Taliban, suggesting that they be recognized as a legal, political party and that Taliban prisoners be released.[190] The offer was quite favorable to the Taliban, and the Afghan population supported it because it involved a negotiated settlement.[191] On February 29, 2020, the United

[178] Guardian Staff, *Bush Rejects Taliban Offer to Hand Bin Laden Over*, THE GUARDIAN (Oct. 14, 2001), *available at* https://www.theguardian.com/world/2001/oct/14/afghanistan.terrorism5.
[179] Michael Moran, *The 'Airlift of Evil'*, NBC NEWS (Dec. 10, 2003), *available at* https://www.nbcnews.com/id/wbna3340165/.
[180] AHMED RASHID, DESCENT INTO CHAOS: THE UNITED STATES AND THE FAILURE OF NATION BUILDING IN PAKISTAN, AFGHANISTAN, AND CENTRAL ASIA. UNITED STATES, (Viking Press 2008).
[181] Editors of Encyclopedia Britannica, *Hamid Karzai: President of Afghanistan*, ENCYCLOPEDIA BRITANNICA (Dec. 20, 2021), *available at* https://www.britannica.com/biography/Hamid-Karzai.
[182] Julian Borger, *Bonn Conference Could Mark Formal Start of Afghan Peace Process*, THE GUARDIAN (Jun. 20, 2011), *available at* https://www.theguardian.com/world/julian-borger-global-security-blog/2011/jun/20/afghanistan-taliban-talks-bonn.
[183] Scott Baldauf, & Owais Tohid, *Taliban Appears to Be Regrouped and Well Funded*, THE CHRISTIAN SCIENCE MONITOR (May 8, 2003), *available at* http://www.csmonitor.com/2003/0508/p01s02-wosc.html.
[184] Pamela Constable, *U.S. Troops Fired at Mob After Kabul Accident*, THE SPOKESMAN-REVIEW (Jun. 6, 2006), *available at* https://www.spokesman.com/stories/2006/jun/01/us-troops-fired-at-mob-after-kabul-accident/.
[185] Saeed Ali Achakzai, *Taliban Reject Afghan President's Peace Talk Offer*, REUTERS (Sep. 30, 2007), *available at* https://www.reuters.com/article/us-afghan-talks-idUSISL26606720070930.
[186] Gareth Porter, *US Silent on Taliban's al-Qaeda Offer*, SOUTH ASIA (Dec. 17, 2009), *available at* https://web.archive.org/web/20091219213931/http://www.atimes.com/atimes/South_Asia/KL17Df02.html.
[187] Olivier Laurent, *When War Is Just Another Day in Afghanistan*, TIME (Jul. 8, 2016), *available at* https://time.com/4402071/afghanistan-war-everyday/.
[188] Ryan Browne, *Carter visits Afghanistan as Obama Plans Handoff of 15-Year War*, CABLE NEWS NETWORK (CNN) (Dec. 9, 2016), *available at* https://edition.cnn.com/2016/12/09/politics/ash-carter-afghanistan-visit/index.html.
[189] James Griffiths, *Trump Calls Out Pakistan, India as He Pledges to 'Fight to Win' in Afghanistan*, CABLE NEWS NETWORK (CNN) (Aug. 24, 2017), *available at* https://edition.cnn.com/2017/08/21/politics/trump-afghanistan-pakistan-india/index.html.
[190] James Rothwell, Mohammad Zubair Khan, & Bilal Sarwary, *Taliban Holds 'Informal' Talks with Afghanistan*, THE TELEGRAPH (Oct. 18, 2016), *available at* https://www.telegraph.co.uk/news/2016/10/18/taliban-holds-informal-peace-talks-with-afghanistan/.
[191] *Id.*

States and the Taliban signed a peace agreement entitled the *Agreement for Bringing Peace to Afghanistan* in Doha, Qatar, where all American and NATO troops leave Afghanistan and the Taliban would not permit Al Qaeda to operate within the country.[192]

AMERICAN DEPARTURE FROM AFGHANISTAN (2021)

The American and NATO departure from Afghanistan was anything but orderly. Between March 1, 2020, and April 15, 2020, the Taliban conducted more than 4,500 attacks in the 45 days after signing the agreement.[193] As of July 23, 2021, the Taliban controlled more than half of Afghanistan's districts.[194] By mid-August 2021, the Taliban controlled all major cities in Afghanistan, including Kabul and the Presidential Palace. President Ashraf Ghani fled to the United Arab Emirates (UAE), where he was given asylum, as confirmed by the UAE Ministry of Foreign Affairs and International Cooperation on August 18, 2021.[195] The remaining Afghan forces under Amrullas Saleh, Amhad Massoud, and Bismillah Khan Mohammadi retreated to the northern province of Panjshir to continue to fight against the Taliban.[196]

The American withdrawal from Afghanistan was chaotic. In mid-April 2020, President Biden proclaimed mission accomplished in Afghanistan and that all American troops would leave the country by September 11, 2020, nineteen years to the day that a terrorist attack destroyed the World Trade Center.[197] President Biden later moved up the departure date to August 31, 2020.[198] President Biden also said that after approximately 20 years of war, the United States military could not transform Afghanistan into a stable democracy.[199]

At night on July 1, 2020, the United States military left the Bagram Air Base in Afghanistan without alerting the base's new Afghan commander.[200] The new commander discovered the American departure more than two hours later.[201] The other airport in Kabul was the Hamid Karzai International Airport which was not defensible from attack, in contrast to the Bagram Air Base, which was abandoned. There was a public outcry from Democrats and Republicans alike regarding how President Biden had withdrawn the troops.[202] The result was that there was no mass evacuation of Afghanistan of the Afghan people who had helped the United States.[203] According to Brufke, between 10,000 and 40,000 Americans were living in Afghanistan at the time.[204] During the six weeks leading up to the American withdrawal from Afghanistan on August 31, 2020, approximately 124,000 Americans and others were evacuated from Afghanistan.[205]

---

[192] Shereena Qazi, *Afghanistan's Taliban, US Sign Agreement Aimed at Ending War*, AL JAZEERA (Feb. 29, 2020), available at https://www.aljazeera.com/news/2020/2/29/afghanistans-taliban-us-sign-agreement-aimed-at-ending-war.

[193] Hamid Shalizi, Abdul Qadir Sediqi, Rupam Jain, *Taliban Step Up Attacks on Afghan Forces Since Signing U.S. Deal: Data*, REUTERS (May 1, 2020), *available at* https://www.reuters.com/article/us-health-coronavirus-afghanistan-taliba/taliban-step-up-attacks-on-afghan-forces-since-signing-u-s-deal-data-idUSKBN22D5S7.

[194] Bill Roggio, *Taliban Squeezes Afghan Government by Seizing Key Border Towns*, FDD'S LONG WAR JOURNAL (Jul. 9, 2021), *available at* https://www.longwarjournal.org/archives/2021/07/taliban-squeezes-afghan-government-by-seizing-key-border-towns.php.

[195] Ava Batrway, *Afghan President Latest Leader on the Run to Turn Up in UAE*, ASSOCIATED PRESS NEWS (Aug. 19, 2021), available at https://apnews.com/article/europe-middle-east-39610b0102a926c1a573da3d6feb0eea.

[196] Emma Graham-Harrison, *'Panjshir Stands Strong': Afghanistan's Last Holdout Against the Taliban*, THE GUARDIAN (Aug. 18, 2021), *available at* https://www.theguardian.com/world/2021/aug/18/panjshir-stands-strong-afghanistans-last-holdout-against-the-taliban.

[197] David Zucchino, *The U.S. War in Afghanistan: How It Started, and How It Ended*, THE NEW YORK TIMES (Oct. 7, 2021), *available at* https://www.nytimes.com/article/afghanistan-war-us.html.

[198] *Id.*

[199] *Id.*

[200] John McCormack, *Why Did the United States Abandon Bagram Airfield?*, NATIONAL REVIEW (Aug. 18, 2021), *available at* https://www.nationalreview.com/2021/08/why-did-the-united-states-abandon-bagram-airfield/.

[201] *Id.*

[202] Barbara Sprunt, *There's A Bipartisan Backlash To How Biden Handled The Withdrawal From Afghanistan*, NATIONAL PUBLIC RADIO (Aug. 17, 2021), *available at* https://www.npr.org/2021/08/16/1028081817/congressional-reaction-to-bidens-afghanistan-withdrawal-has-been-scathing.

[203] Zolan Kanno-Youngs, & Annie Karni, *Series of U.S. Actions Left Afghan Allies Frantic, Stranded and Eager to Get Out*, THE NEW YORK TIMES (Aug. 29, 2021), *available at* https://www.nytimes.com/2021/08/18/us/politics/afghanistan-refugees.html.

[204] Juliegrace Brufke, *supra*, note 122.

[205] Associated Press, *EXPLAINER: What Happened to the Afghanistan Evacuation?*, U.S. NEWS AND WORLD REPORT (Nov. 26, 2021), *available at* https://www.usnews.com/news/politics/articles/2021-11-26/explainer-what-happened-to-the-afghanistan-evacuation.

In Light of The American Departure From Afghanistan, Does Network-Centric Warfare Adequately Prepare The United States to Address Future Cyber Activities by The Taliban?

After August 31, 2020, there has only been a trickle of people leaving Afghanistan.[206] One result of the American departure is that critics of the withdrawal proclaimed that the United States left approximately $83 billion was spent in Afghanistan.[207] Kessler observed that only $75 billion of the $83 billion had been dispersed from 2002 to June 30, 2021.[208] Not all of the money that was dispersed was spent on military equipment.[209] President Biden justified the withdrawal when he said that he did not see a way to leave Afghanistan without some amount of chaos resulting from the withdrawal.[210] Even so, some of President Biden's critics in Congress and the media disagreed with the assessment.[211]

SECOND ISLAMIC EMIRATE OF AFGHANISTAN (2021 AND BEYOND)

As of the writing of this article, the second Islamic Emirate of Afghanistan is a reality. In an interview, Lucas and Rafi aptly observed that the Taliban is not a homogeneous organization.[212] Some parts of the Taliban want the organization to rule Afghanistan in the light of modern realities, whereas other parts of the Taliban want to return to the Taliban policies of the 1990s.[213] How this conflict will play out in the future is an open question. One thing is for sure. With the exodus of tens of thousands of Afghans, it is unlikely that the Taliban will have the expertise to create an effective government, at least in the short term.

In the Taliban's efforts to remove the Islamic State from the country, their efforts have become increasingly brutal.[214] According to Clarke and Schroden, suspected members of the Islamic State have been hung in public or beheaded.[215] These tactics are ruthless, but the question is whether these practices are working.[216] The Taliban's current issue is forming an effective government, ensuring stability, and addressing a collapsing economy and ever-decreasing social services.[217] The problem facing the Taliban is transforming itself from an insurgency organization into a governing body.

The longer it takes the Taliban to defeat the insurgent Islamic State, the greater the threat to its newfound position as rulers of Afghanistan.[218] The Islamic State may posture itself as a jihadist movement and a government. The other issue confronting the Taliban is that the more time and resources they expend on the Islamic State, the fewer time and resources the Taliban have to create a government. According to Clarke and Schroden, the Taliban may be forced by circumstances to modify their approach to the Islamic State to avoid an economic collapse.[219] The Taliban will have to decide what to do and the means for achieving what they want to happen.

IS THE UNITED STATES OF AMERICA ADEQUATELY PREPARED?

This section of the paper is divided by the different types of organizations and their preparedness for a cyber attack. However, before addressing the various categories of institutions from a cyber perspective, it is essential to understand what it means to be prepared adequately from a network-centric point of view.

---

[206] *Id.*

[207] Glenn Kessler, *No, the Taliban Did Not Seize $85 Billion of U.S. Weapons*, THE WASHINGTON POST (Aug. 31, 2021), *available at* https://www.washingtonpost.com/politics/2021/08/31/no-taliban-did-not-seize-83-billion-us-weapons/.

[208] SIGAR Staff, *Section 2 Reconstruction Update*, SPECIAL INSPECTOR GENERAL FOR AFGHANISTAN RECONSTRUCTION 29 (Jul. 30, 2021), available at https://www.sigar.mil/pdf/quarterlyreports/2021-07-30qr-section2-funding.pdf#Page=9.

[209] Glenn Kessler, *supra*, note 207.

[210] Zolan Kanno-Youngs, & Annie Karni, *supra*, note 203.

[211] *Id.*

[212] Converstation Staff, *What's Next for Afghanistan? Two Experts Make Predictions*, THE CONVERSATION (Nov. 30, 2021), *available at* https://theconversation.com/whats-next-for-afghanistan-two-experts-make-predictions-170684.

[213] *Id.*

[214] Colin Clarke, & Jonathan Schroden, *Brutally Ineffective: How the Taliban Are Failing in Their New Role as Counter-Insurgents*, WAR ON THE ROCKS (Nov. 19, 2021), *available at* https://warontherocks.com/2021/11/brutally-ineffective-how-the-taliban-are-failing-in-their-new-role-as-counter-insurgents/.

[215] *Id.*

[216] *Id.*

[217] *Id.*

[218] *Id.*

[219] *Id.*

MEANING OF ADEQUATE PREPARATION

The Boy Scout motto is: "Be Prepared!"[220] Adequate preparation means that one is in a state of readiness to perform a particular act.[221] Adequate preparedness is being as suitable as necessary for a specific requirement or purpose.[222] The term can also be interpreted to mean barely sufficient, appropriate, or acceptable.[223] In the law, adequate preparedness is equivalent to being reasonably able to begin legal action.[224] Regarding cyber operations, proper preparation implies that a country, corporation, or individual can effectively ward off a cyberattack while at the same time suffering a fraction of cyber damages.[225]

ADEQUATE PREPARATION FOR INDIVIDUALS

Individuals are natural persons that typically lack the financial resources to purchase extensive protection of their computers and cyber assets. Individuals usually buy off-the-shelf Internet security packages such as Norton Anti-Virus, McAfee Total Protection, or Kaspersky Total Security. These security packages cost less than $200.00 and are within the budgets of most individual users. Of course, some cybersecurity packages are better than others because an application can detect unwarranted intrusions and then nullify the adverse effects of the malware.

Individuals are at the mercy of the software security systems they buy for their computers regarding cyber espionage, cyber terrorism, and cyber warfare. A genuine issue for individuals is that with the advent of the Internet of Things, many products today that connect to the Internet are sorely lacking in cybersecurity. For example, computer systems whose purpose is to monitor babies when left alone in their rooms have been known to be hijacked by malicious hackers who intend to disrupt the lives of the child's parents. Another example is the burgeoning use of intelligent assistants such as Amazon's Echo or Google's Home companions. These Internet-connected devices are becoming prevalent in people's homes and with little or no programmed cybersecurity applications. Cybercriminals or even cyber joyriders can potentially hack these machines.

A third example is smartphones. Edward Snowden was recently interviewed, wherewith the use of an international mobile subscriber identity-catcher (IMSI-catcher), he was able to turn on the front and rear cameras, as well as the microphone of a cell phone that was in possession of a Vice reporter, located 6,000 miles away from Russia where Snowden was residing.[226] The reporter's cell phone was physically turned off at the time.[227] The interview demonstrated quite vividly that a user could never really turn off many cell phones unless the individual physically removes the battery from the device.[228] In other words, if there is no power, there is no signal and hence no transmission or reception of data.[229]

ADEQUATE PREPARATION FOR COMPANIES AND CORPORATIONS

Cybersecurity is anathema to companies. Although corporations have no desire to have their records hacked or stolen by foreign governments or other corporations as part of a corporate espionage effort, American companies have expressed their unwillingness to share their cyber detection and intrusion information with federal, state, and local governments. The reason is that once it is acknowledged that a company has been hacked and its records have been stolen, an organization typically suffers a temporary and sometimes permanent decline in its stock price. In the United States, since *Dodge v. Ford Motor Company* was decided nearly a century ago, the purpose of a corporation is to maximize shareholder value.[230] In simple terms, it means to ensure that a company's stock price does not drop dramatically for any reason. Of course, stocks can decline for business reasons, but a cyber attack is not a business reason in any sense of the word.

---

[220] *Boy Scout Oath, Law, Motto and Slogan and the Outdoor Code*, US SCOUTING SERVICE PROJECT (n.d.), *available at* http://usscouts.org/advance/ScoutsBSA/oathlaw.asp. The Boy Scout web site contains the changes made to the principles of Scouting after January 01, 2019.

[221] *See generally*, *Adequate Prepardedness*, MERRIAM-WEBSTER DICTIONARY (n.d.), *available at* https://www.merriam-webster.com/dictionary/preparedness.

[222] *Id*.

[223] *See generally*, *Adequate Prepardedness*, THE LAW DICTIONARY FEATURING BLACK'S LAW DICTIONARY (n.d.), *available at* https://thelawdictionary.org/adequate-preparation/.

[224] *Id*.

[225] The Cadmus Group LLC, *Cybersecurity Prepardedness Evaluation Tool*, NATIONAL ASSOCIATION OF REGULATORY UNITITY COMMISSIONERS (Jun. 2019), *available at* https://pubs.naruc.org/pub/3B93F1D2-BF62-E6BB-5107-E1A030CF09A0.

[226] *'State of Surveillance' with Edward Snowden and Shane Smith (VICE on HBO: Season 4, Episode 13)*, YOUTUBE.COM (January 08, 2016), *available at* https://www.youtube.com/watch?v=ucRWyGKBVzo.

[227] *Id*.

[228] *Id*.

[229] *Id*.

[230] *Dodge v. Ford Motor Company*, 204 Mich. 459 (1919).

The practical effect of such shortsightedness is that many companies have suffered cyber attacks of mammoth proportions. Firms such as Marriot Hotels, Target, Home Depot, Equifax, Delta Airlines, Best Buy, FedEx, K-Mart, Sears & Roebuck, Macy's, just to name a few, have all been victims of cyber attacks in the recent past. Based on various analyses of these attacks, it is readily apparent that American companies are woefully unprepared to deal effectively with adverse cyber operations. The primary reason why these companies are the target of cyberattacks is apparent. These firms are bastions of economic and financial data of customer information. It is like robbing a bank. The reason to rob a bank is that a bank is where the money is. Similarly, confidential personal information of customers has monetary value, and hence from a hacker's perspective, it makes good economic sense to attack major American corporations.

Why does a corporation not vigorously act to protect its data? The reasons are deeply rooted in *Dodge v. Ford*.[231] The purpose of a company is to maximize shareholder value, or in economic terms, to maximize profits. Some senior executives do not necessarily appreciate that profit maximization is logically equivalent to cost minimization. Because companies do not readily perceive increased earnings from investing in cybersecurity, the activity usually plays second fiddle to more profit-making behaviors such as introducing, marketing and selling new or existing products.

This lack of forethought can be freely observed when examining products' security features, commonly known as the Internet of Things (IoT). The security software is typically stamped into the device where the individual owner does not have the technical expertise to change default passwords or implement additional safeguards, or the machine is merely devoid of a mechanism to make the appropriate security changes. The result is that Internet-connected devices are fast becoming like walking zombies, ready, willing, and able to do the bidding of their hacking masters.

ADEQUATE PREPARATION FOR GOVERNMENTS

The problem with determining whether governments are adequately prepared to cope with cyber operations is that once a government discloses to the public that it can repel a cyberattack, its ability to fend off a future attack is severely compromised. An opponent, albeit a private organization or a nation-state, can glean valuable information from the fact that a country has successfully mitigated a cyber attack. The truth is that only government officials with the need to know have the requisite knowledge to categorically state whether their country is adequately prepared to address an adverse cyber operation. Citizens of nations are rarely if ever, privy to state secrets. Governments must impose the utmost secrecy regarding their cyber operational capability regarding cyberattacks. This author cannot answer whether the United States government is adequately prepared because he lacks the necessary security clearance. Even if this author had the security clearance to answer the question affirmatively, it would be a felony to do so, resulting in years of imprisonment in a federal correctional facility. With that said, it is a sincere hope that the United States has prepared much more than adequate to combat any future cyber-attack, given that it spends over $700 billion annually on military expenditures.

CONCLUSION

The issue under consideration was whether network-centric warfare has adequately prepared the United States to deal with the cyber activities of the Taliban. Currently, the Taliban is consolidating their political power in Afghanistan, where their apparent major rival is the Islamic State. Another rival to the Taliban is the forces under Amrullas Saleh, Amhad Massoud, and Bismillah Khan Mohammadi in the northern province of Panjshir. Likely, the Taliban does not pose a cyber threat to the United States in the short term. On the other hand, as the Taliban consolidate their power within Afghanistan, there is a probability that technically savvy members of the organization will engage in cyber activities against the United States. This situation implies that individuals, corporations, and the state and federal governments have breathing room to improve their preparedness. Whether they take this time to solidify their preparedness is an open question. It can be safely presumed that some organizations will prepare thoroughly, some entities will prepare adequately, some groups will prepare minimally, and some persons (natural or otherwise) will not prepare at all.

Will the Taliban attack the United States employing cyber tools? In this world of the Internet, the one sure thing is that a cyber-attack can come from anywhere. Thus, constant vigilance is the order of the day. Nothing short of this will suffice.

REFERENCES:

1) Lindsay Maizland, The Taliban in Afghanistan, THE COUNCIL OF FOREIGN RELATIONS (Sep. 15, 2021), available at https://www.cfr.org/backgrounder/taliban-afghanistan.
2) Press Release, SEN. MARCO RUBIO, Rubio Introduces Bill to Designate Taliban As a Foreign Terrorist Organization (Sep. 15, 2021), https://www.rubio.senate.gov/public/index.cfm/2021/9/rubio-introduces-bill-to-designate-taliban-as-a-foreign-terrorist-organization.

[231] *Id.*

3) MICHAEL N. SCHMITT (GEN. ED.), TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Cambridge University Press 2017).
4) RICHARD A. CLARKE, & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT (HarperCollins Publishers 2010).
5) Patrick Clark, The Hotel Hackers Are Hiding in the Remote Control Curtains, BLOOMBERG BUSINESSWEEK (Jun. 26, 2019), available at https://www.bloomberg.com/news/features/2019-06-26/the-hotel-hackers-are-hiding-in-the-remote-control-curtains.
6) JENS DAVID OHLIN, KEVIN GOVERN, & CLAIRE FINKELSTEIN, CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS (Oxford University Press 2015).
7) UNITED STATES DEPARTMENT OF DEFENSE, LAW OF ARMED CONFLICT DESKBOOK (CreateSpace Independent Publishing Platform 16th ed. Aug. 17, 2018).
8) Jens David Ohlin, Kevin Govern, & Claire Finkelstein, supra, note 11.
9) Donald L. Buresh, Russian Cyber-Attacks on Estonia, Georgia, and Ukraine Including Tactics, Techniques, Procedures, and Effects, 1 JOURNAL OF ADVANCED FORENSIC SCIENCES 2, 15-26 (Aug. 2021), available at DOI: 10.14302/issn.2692-5915.jafs-21-3930.
10) LIANG QIAO, & XIANGSUI WANG, UN-RESTRICTED WARFARE (Echo Point Books & Media 1999).
11) Jens David Ohlin, Kevin Govern, & Claire Finkelstein, supra, note 11.
12) THOMAS RID, CYBER WAR WILL NOT TAKE PLACE (Oxford University Press 2013).
13) Michael A. Warren, (Nov. 2010) (unpublished Master of Science thesis, Ohio University), available at https://etd.ohiolink.edu/apexprod/rws_etd/send_file/send?accession=ohiou1289446353&disposition=inline.
14) Thomas Rid, supra, note 18.
15) Parliamentary Office Staff, Assessing the Risk of Terrorist Attacks on Nuclear Facilities, PARLIAMENTARY OFFICE OF SCIENCE AND TECHNOLOGY (Jul. 2004), available at https://www.parliament.uk/globalassets/documents/post/postpr222.pdf.
16) Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, & Julia Spiegel, The Law of Cyber Attack, 100 CALIFORNIA LAW REVIEW 4, 817-85 (Aug. 2012), available at https://www.jstor.org/stable/23249823.
17) Thomas Rid, supra, note 18.
18) Catalin Cimpanu, New Iranian Data Wiper Malware Hits Bapco, Bahrain's National Oil Company, ZDNET (Jan. 09, 2020), available at https://www.zdnet.com/article/new-iranian-data-wiper-malware-hits-bapco-bahrains-national-oil-company/.
19) Thomas Rid, supra, note 16.
20) NIST Staff, Red Team, COMPUTER SECURITY RESOURCE CENTER (n.d.), available at https://csrc.nist.gov/glossary/term/red_team.
21) Thomas Rid, supra, note 18.
22) Id.
23) ROBERT W. TAYLOR, TORI J. CAETI, D. KALL LOPER, ERIC J. FRITSCH, & JOHN LIEDERBACH, DIGITAL CRIME AND DIGITAL TERRORISM (Pearson Education, Inc. 2006).
24) Peter W. Singer, The Cyber Terror Bogeyman, BROOKINGS INSTITUTE (Nov. 01, 2012), available at https://www.brookings.edu/articles/the-cyber-terror-bogeyman/.
25) Marin Ivezic, The World of Cyber-Physical Systems & Rising Cyber-Kinetic Risks, MARIN IVEZIC (Mar. 31, 2015), available at https://cyberkinetic.com/cyber-kinetic-security/cyber-kinetic-risks/.
26) HEDIEH NASHERI, ECONOMIC ESPIONAGE AND INDUSTRIAL SPYING (Cambridge University Press 2005).
27) Lee Rainie, Janna Anderson, & Jennifer Connolly, Cyber Attacks Likely to Increase, PEW RESEARCH CENTER (Oct. 29, 2014), available at https://www.pewresearch.org/internet/2014/10/29/cyber-attacks-likely-to-increase/.
28) BRANDON VALERIANO, & RYAN C. MANESS, CYBER WAR VERSUS CYBER REALITIES: CYBER CONFLICT IN THE INTERNATIONAL SYSTEM (Oxford University Press 2015).
29) Foreign Cyber Threats to the United States, HEARING BEFORE THE COMMITTEE ON ARMED SERVICES: UNITED STATES SENATE ONE HUNDRED FIFTEENTH CONGRESS FIRST SESSION (Jan. 05, 2017), available at https://www.govinfo.gov/content/pkg/CHRG-115shrg33940/html/CHRG-115shrg33940.htm.
30) Donald L. Buresh, A Critical Evaluation of the Estonian Cyber Incident, 1 JOURNAL OF ADVANCED FORENSIC SCIENCES 2, 7-14 (Nov. 03, 2020), available at DOI 10.14302/issn.2692-5915.jafs-20-3601.
31) Michael N. Schmitt, supra, note 3.

32) RICHARD STIENNON, THERE WILL BE CYBERWAR: HOW TO MOVE TO NETWORK-CENTRIC WARFIGHTING SET THE STAGE FOR CYBERWAR (IT-Harvard Press 2015).
33) Richard A. Clarke, & Robert K. Knake, supra, note 6.
34) Thomas Rid, supra, note 18.
35) Matthew Weaver, Teenage Hackers Motivated by Morality Not Money, Study Finds, THE GUARDIAN (Apr. 21, 2017), available at https://www.theguardian.com/society/2017/apr/21/teenage-hackers-motivated-moral-crusade-money-cybercrime.
36) SUSAN W. BRENNER, CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE (Praeger 2010).
37) Jens David Ohlin, Kevin Govern, & Claire Finkelstein, supra, note 11.
38) Darien Pun, Rethinking Espionage in the Modern Era, 18 CHICAGO JOURNAL OF INTERNATIONAL LAW. 1, 353-91 (Jul. 2017), available at https://chicagounbound.uchicago.edu/cjil/vol18/iss1/10/.
39) Thomas Rid, supra, note 18.
40) Alex Schmid, Terrorism - The Definitional Problem, 36 CASE WESTERN RESERVE JOURNAL OF INTERNATIONAL LAW 2, 375-419 (2004), available at https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1400&context=jil.
41) Matthew J. Littleton, INFORMATION AGE TERRORISM: TOWARD CYBERTERROR, (Dec. 1995) (unpublished Master of Science thesis, Naval Postgraduate School), available at https://fas.org/irp/threat/cyber/docs/npgs/terror.htm#TOC.
42) FRED KAPLAN, DARK TERRITORY: THE SECRET HISTORY OF CYBER WAR (Simon & Schuster 2016).
43) Thomas Rid, supra, note 18.
44) Shamsuddin Abdul Jalil, Countering Cyber Terrorism Effectively: Are We Ready To Rumble?, SANS INSTITUTE (Jun. 2003), available at https://www.giac.org/paper/gsec/3108/countering-cyber terrorism-effectively-ready-rumble/105154#:~:text=The%20most%20common%20objective%20of,on%20particular%20targets%20%5B2%5D.
45) Jordan Robertson, Is There Really a Cyberwar? Term Might Be Misused, PHYS.ORG (May 05, 2010), available at https://phys.org/news/2010-05-cyberwar-term-misused.html.
46) Chris Colvin, Daniel B. Garrie, & Siddartha Rao, Cyber Warfare and the Corporate Environment, 2 JOURNAL OF LAW & CYBER WARFARE 1, 1-24 (Spring 2013), available at https://www.jstor.org/stable/26441239.
47) Paul Strassman, Asymmetric Cyberwarfare Demands a New Information Assurance Approach, ARMED FORCES COMMUNICATIONS AND ELECTRONICS ASSOCIATION (Jul. 01, 2013), available at https://www.afcea.org/content/asymmetric-cyberwarfare-demands-new-information-assurance-approach.
48) Chris Colvin, Daniel B. Garrie, & Siddartha Rao, supra, note 73.
49) FREDERICK A. HAYEK, LAW, LEGISLATION AND LIBERTY: A NEW STATEMENT OF THE LIBERAL PRINCIPLES OF JUSTICE AND POLITICAL ECONOMY (Routledge Classics 2012).
50) William Owens, The Emerging U.S. System of Systems, INSTITUTE FOR NATIONAL STRATEGIC STUDIES, 63 (Feb. 1996), available at http://www.dtic.mil/get-tr-doc/pdf?AD=ADA394313.
51) Corporate Initiatives Group, C4ISR Forward . . . A Vision of the Future. SAN DIEGO, CALIFORNIA: NAVAL COMMAND (Jul. 1997), available at https://www.dtic.mil/dtic/tr/fulltext/u2/a434155.pdf.
52) Arthur K. Cebrowski, & John H. Garstka, Network-Centric Warfare - Its Origin and Future, UNITED STATES NAVAL INSTITUTE (Jan. 1998), available at https://www.usni.org/magazines/proceedings/1998/january/network-centric-warfare-its-origin-and-future.
53) DAVID ALBERTS, JOHN GARSTKA, & FREDERICK STEIN, NETWORK CENTRIC WARFARE: DEVELOPING AND LEVERAGING INFORMATION SUPERIORITY (Department of Defense: Command and Control Research Program 2nd. ed. 2003), available at http://www.dodccrp.org/files/Alberts_NCW.pdf.
54) DAVID ALBERTS, JOHN GARSTKA, RICHARD HAYES, R., & DAVID A. SIGNORI, UNDERSTANDING INFORMATION AGE WARFARE (Department of Defense: Command and Control Research Program 2001), available at https://www.voltairenet.org/IMG/pdf/Understanding_Information_Age_Warfare-2.pdf.
55) DAVID ALBERTS, JOHN GARSTKA, RICHARD HAYES, R., & DAVID A. SIGNORI, UNDERSTANDING INFORMATION AGE WARFARE (Department of Defense: Command and Control Research Program 2001), available at https://www.voltairenet.org/IMG/pdf/Understanding_Information_Age_Warfare-2.pdf.
56) DAVID S. ALBERTS, INFORMATION AGE TRANSFORMATION: GETTING TO A 21ST CENTURY MILITARY (Department of Defense: Command and Control Research Program 2002), available at http://dodccrp.org/files/Alberts_IAT.pdf
57) MARIUS VASSILIOU, DAVID S. ALBERTS, & JONATHAN R. AGRE, C2 RE-ENVISIONED: THE FUTURE OF THE ENTERPRISE (Chemical Rubber Company Press 2015).

58) Clay Wilson, Network Centric Operations: Background and Oversight Issues for Congress, CONGRESSIONAL RESEARCH SERVICE (Mar. 15, 2007), available at https://www.researchgate.net/publication/235121618_Network_Centric_Operations_Background_and_Oversight_Issues_for_Congress.
59) MICHAEL E. WHITMAN, & HERBERT J. MATTORD, PRINCIPLES OF INFORMATION SECURITY (Cengage Learning 2016).
60) Gustavus J. Simmons, Symmetric and Asymmetric Encryption, 11 ACM COMPUTING SURVEYS 4, 305-30 (Dec. 1979), available at https://doi.org/10.1145/356789.356793.
61) Id.
62) RYAN RUSSELL, TIMOTHY MULLEN, & JOHNNY LONG, STEALING THE NETWORK: THE COMPLETE SERIES COLLECTOR'S EDITION (Elsevier Publishing 2009), available at https://books.google.com/books?id=4csyeZaEP4cC&pg=PA651&lpg=PA651&dq=stealing+a+computer+that+uses+asymmetric+encryption&source=bl&ots=tJLyiwwBiI&sig=ACfU3U1y2COvwBkp5fsPZwhdcuYDacPSww&hl=en&sa=X&ved=2ahUKEwjbzs2kwrbyAhWKbs0KHXU3Ck4Q6AF6BAg5EAM#v=onepage&q=stealing%20a%20computer%20that%20uses%20asymmetric%20encryption&f=false.
63) DAVID MOWRY, GERMAN CIPHER MACHINES OF WORLD WAR II (National Security Agency: Center for Cryptologic History rev. ed. 20014), available at https://www.nsa.gov/Portals/70/documents/about/cryptologic-heritage/historical-figures-publications/publications/wwii/german_cipher.pdf.
64) Gustavus J. Simmons, supra, note 97.
65) Henry Kamradt, & Douglas MacDonald, The Implications of Network-Centric Warfare for United States and Multinational Military Operations, UNITED STATES NAVAL WAR COLLEGE (Dec. 31, 1998), available at https://apps.dtic.mil/sti/pdfs/ADA430553.pdf.
66) Clay Wilson, supra, note 90.
67) KIMBERLY S. YOUNG, & CRISTIANO NABUCO, DE ABREU (EDS.), INTERNET ADDICTION: A HANDBOOK AND GUIDE TO EVALUATION AND TREATMENT (John Wiley & Sons, Inc. 2011), available at http://www.ssu.ac.ir/cms/fileadmin/user_upload/Moavenatha/MBehdashti/ravan/pdf/faaliyatha/pptfiles/INTERNET_ADDICTION.pdf#page=39
68) Henry Kamradt, & Douglas MacDonald, supra, note 102.
69) Joseph H. Scherrer, Risks and Vulnerabilities of Network-Centric Forces: Insights from the Science of Complexity, NAVAL WAR COLLEGE (Feb. 03, 2003), available at https://apps.dtic.mil/sti/citations/ADA415474.
70) Clay Wilson, supra, note 90.
71) David L. Peeler, Jr., & Michael P. Dahlstrom, Network Centric Warfare: Advantages and Disadvantages, STRATEGIC IMPACT NO. 3 (2003), available at https://www.proquest.com/openview/364a2a648a2241267b93979755e55788/1?pq-origsite=gscholar&cbl=1876337.
72) Joseph H. Scherrer, supra, note 113.
73) Clay Wilson, supra, note 90.
74) David L. Peeler, Jr., & Michael P. Dahlstrom, supra, note 115.
75) Terri Moon Cronk, Biden Announces Full U.S. Troop Withdrawal from Afghanistan by Sept. 11, UNITED STATES DEPARTMENT OF DEFENSE (Apr. 14, 2021), available at https://www.defense.gov/Explore/News/Article/Article/2573268/biden-announces-full-us-troop-withdrawal-from-afghanistan-by-sept-11/.
76) Madeleine Ngo, Biden Defends Decision to Pull Out of Afghanistan, THE NEW YORK TIMES (Aug. 18, 2021), available at https://www.nytimes.com/live/2021/08/16/us/politics-news.
77) Paul D. Shrinkman, Chaos, Violence at Kabul Airport as U.S. Tries to Complete Afghanistan Evacuation, U.S. NEWS & WORLD REPORT (Aug. 16, 2021), available at https://www.usnews.com/news/world-report/articles/2021-08-16/chaos-violence-at-kabul-airport-as-us-tries-to-complete-afghanistan-evacuation.
78) Juliegrace Brufke, Biden team vague on evacuating Americans, allies from Afghanistan after Aug. 31, THE NEW YORK POST (Aug. 17, 2021), available at https://nypost.com/2021/08/17/biden-team-vague-on-evacuating-americans-allies-from-afghanistan/.
79) Mark Moore, David Petraeus calls Afghanistan a 'Dunkirk Moment', THE NEW YORK POST (Aug. 17, 2021), available at https://nypost.com/2021/08/17/david-petraeus-calls-afghanistan-a-dunkirk-moment/.
80) Miriam Jordan, Thousands Who Helped the U.S. in Afghanistan Are Trapped. What Happens Next?, THE NEW YORK TIMES (Aug. 16, 2021), available at https://www.nytimes.com/2021/08/16/us/afghanistan-visa-refugees-us.html.

81) Robert Clark, As NATO Allies Flounder, British Troops Are Leading by Example at Kabul Airport, THE TELEGRAPH (Aug. 18, 2021), available at https://www.telegraph.co.uk/news/2021/08/19/nato-allies-flounder-british-troops-leading-example-kabul-airport/.
82) James R. Webb, As US Military Sticks to Airport, British and French Forces Are Rescuing their Citizens in Kabul: Reports, MILITARY TIMES (Aug. 19, 2021), available at https://www.militarytimes.com/flashpoints/afghanistan/2021/08/19/as-us-military-sticks-to-airport-british-and-french-forces-are-rescuing-their-citizens-in-kabul-reports/.
83) Loveday Morris, Amid Sharp Criticism, Germany Stumbles in Late Efforts to Rescue Afghan Support Staff, THE WASHINGTON POST (Aug. 22, 2021), available at https://www.washingtonpost.com/world/germany-afghans-evacuation/2021/08/21/d33941ce-0202-11ec-ba7e-2cf966e88e93_story.html.
84) Robert Fife, Canadian special forces may be used to rescue Afghan interpreters, support staff from Kabul: Sajjan, THE GLOBE AND MAIL (Aug. 22, 2021), available at https://www.theglobeandmail.com/politics/article-canadian-special-forces-may-be-used-to-rescue-afghan-interpreters/.
85) Victor Davis Hanson, Victor Davis Hanson: If Biden were a Republican, Dems in Congress would have impeached him. They should, FOX NEWS (Aug. 22, 2021), available at https://www.foxnews.com/opinion/biden-republican-democrats-congress-impeached-victor-davis-hanson.
86) Ryan Morgan, US Has No Plans to Rescue Americans, Afghans Stranded behind Taliban Lines Outside Kabul A, Airport, AMERICAN MILITARY NEWS (Aug. 18, 2021), available at https://americanmilitarynews.com/2021/08/us-has-no-plans-to-rescue-americans-afghans-stranded-behind-taliban-lines-outside-kabul-airport/.
87) CHRISTOPHER R SMITH, NETWORK CENTRIC WARFARE, COMMAND, AND THE NATURE OF WAR (Land Warfare Studies Centre (Australia) 2010), available at https://researchcentre.army.gov.au/sites/default/files/sp318ncwcommandandnatureofwarchristopher_smith.pdf.
88) PAUL KRUGMAN, & ROBIN WELLS, ECONOMICS (Worth Publishers 5th ed. 2017).
89) Paul Murdock, Principles of War on the Network-Centric Battlefield: Mass and Economy of Force, 32 THE US ARMY WAR COLLEGE QUARTERLY: PARAMETERS 1 (Spring 2002), available at https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=2082&context=parameters.
90) Paul Krugman, & Robin Wells, supra, note 133.
91) JOHN MAYNARD KEYNES, THE GENERAL THEORY OF EMPLOYMENT, INTEREST, AND MONEY (Palgrave Macmillan 1936).
92) Kalpana Jain, The History of the Taliban Is Crucial in Understanding Their Success Now – And Also What Might Happen Next, THE CONVERSATION (Aug. 26, 2021), available at https://theconversation.com/the-history-of-the-taliban-is-crucial-in-understanding-their-success-now-and-also-what-might-happen-next-166630.
93) History.com Editors, Soviet Union InvadesAfghanistan, HISTORY.COM (Nov. 24, 2009), available at https://www.history.com/this-day-in-history/soviet-tanks-roll-into-afghanistan.
94) Kalpana Jain, supra, note 138.
95) Colin Price, Pakistan: A Plethora of Problems, 3 GLOBAL SECURITY STUDIES 1, 53-62 (Winter 2012), available at https://www.semanticscholar.org/paper/Pakistan%3A-A-Plethora-of-Problems-Price/b7c99634746e77be1bfb50346198b5d4779214f5.
96) History.com Editors, supra, note 147.
97) John Sifton, Blood-Stained Hands: Past Atrocities in Kabul and Afghanistan's Legacy of Impunity, HUMAN RIGHTS WATCH (Jul. 6, 2005), available at https://www.hrw.org/report/2005/07/06/blood-stained-hands/past-atrocities-kabul-and-afghanistans-legacy-impunity#.
98) NEAMATOLLAH NOJUMI. THE RISE OF THE TALIBAN IN AFGHANISTAN: MASS MOBILIZATION, CIVIL WAR, AND THE FUTURE OF THE REGION (Palgrave 1st ed. 2002 1st ed.).
99) AMIN SAIKAL, MODERN AFGHANISTAN: A HISTORY OF STRUGGLE AND SURVIVAL (I.B. Tauris & Co.1st ed. 2006).
100) John Sifton, Blood-Stained Hands: Past Atrocities in Kabul and Afghanistan's Legacy of Impunity, HUMAN RIGHTS WATCH (Jul. 6, 2005), available at https://www.hrw.org/report/2005/07/06/blood-stained-hands/past-atrocities-kabul-and-afghanistans-legacy-impunity.
101) AMIN SAIKAL, MODERN AFGHANISTAN: A HISTORY OF STRUGGLE AND SURVIVAL (I. B. Tauris & Co. 2006).
102) Lindsay Maizland, The Taliban in Afghanistan, COUNCIL ON FOREIGN RELATIONS (Sep. 15, 2021), available at https://www.cfr.org/backgrounder/taliban-afghanistan.
103) Robert Nichols, Afghan Historiography: Classical Study, Conventional Narrative, National Polemic, 3 HISTORY COMPASS 1 (Dec 21, 2005), available at https://doi.org/10.1111/j.1478-0542.2005.00141.x.

104) AHMED RASHID, AHMED (2000), TALIBAN: MILITANT ISLAM, OIL AND FUNDAMENTALISM IN CENTRAL ASIA 65 (Yale University Press 2000).
105) Id. at 71.
106) ReliefWeb Staff, MSF and Other Aid Organizations Evicted from Kabul, RELIEFWEB (Jul. 21, 2998), available at https://reliefweb.int/report/afghanistan/msf-and-other-aid-organizations-evicted-kabul.
107) Katherine Haddon, Afghanistan Marks 10 Years Since War Started, YAHOO! NEWS (Oct. 6, 2011), available at https://web.archive.org/web/20111010055026/http://news.yahoo.com/afghanistan-marks-10-years-since-war-started-211711851.html.
108) JEANNE K. GIRALDO, & HAROLD A. TRINKUNAS, TERRORISM FINANCING AND STATE RESPONSES : A COMPARATIVE PERSPECTIVE 96 (Stanford University Press 2007).
109) Ahmed Rashid, supra, note 162.
110) DANIEL BYMAN, DEADLY CONNECTIONS: STATES THAT SPONSOR TERRORISM 195 (Cambridge University Press 2005).
111) EDWARD GIRARDET. KILLING THE CRANES: A REPORTER'S JOURNEY THROUGH THREE DECADES OF WAR IN AFGHANISTAN 416 (Chelsea Green Publishing. 2011).
112) Piotr Balcerowicz, The Last Interview with Ahmad Shah Masood, HOJA BAHAUDDIN (early August 2001), available at https://web.archive.org/web/20060925043421/http://www.orient.uw.edu.pl/balcerowicz/texts/Ahmad_Shah_Masood_en.htm.
113) John F. Burns, Threats And Responses: Assassination; Afghans, Too, Mark a Day of Disaster: A Hero Was Lost, THE NEW YORK TIMES (Sep. 9, 2002), available at https://www.nytimes.com/2002/09/09/world/threats-responses-assassination-afghans-too-mark-day-disaster-hero-was-lost.html.
114) Peter L. Bergen, September 11 Attacks, ENCYCLOPEDIA BRITANNICA (n.d.), available at https://www.britannica.com/event/September-11-attacks.
115) George W. Bush, Text: President Bush Addresses the Nation, THE WASHINGTON POST (Sep.20, 2001) available at https://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bushaddress_092001.html.
116) Press Release, NORTH ATLANTIC TREATY ORGANIZATION, Statement by the North Atlantic Council (Sep. 12, 2001), https://www.nato.int/docu/pr/2001/p01-124e.htm.
117) John F. Burns, A Nation Challenged: Last Chance; Taliban Refuse Quick Decision Over bin Laden, THE NEW YORK TIMES (Sep. 18, 2001), available at https://www.nytimes.com/2001/09/18/world/a-nation-challenged-last-chance-taliban-refuse-quick-decision-over-bin-laden.html.
118) CNN Staff, Afghanistan Wakes After Night of Intense Bombings, CABLE NEWS NETWORK (CNN) (Oct. 7, 2001), available at http://edition.cnn.com/2001/US/10/07/gen.america.under.attack/.
119) George W. Bush, Presidential Statement: Bush Announces Military Action Against Terrorist Infrastructure in Afghanistan, CQ ALMANAC (Oct. 7, 2001), available at https://library.cqpress.com/cqalmanac/document.php?id=cqal01-106-6369-328096.
120) https://www.theguardian.com/world/2001/oct/14/afghanistan.terrorism5.
121) Michael Moran, The 'Airlift of Evil', NBC NEWS (Dec. 10, 2003), available at https://www.nbcnews.com/id/wbna3340165/.
122) AHMED RASHID, DESCENT INTO CHAOS: THE UNITED STATES AND THE FAILURE OF NATION BUILDING IN PAKISTAN, AFGHANISTAN, AND CENTRAL ASIA. UNITED STATES, (Viking Press 2008).
123) Editors of Encyclopedia Britannica, Hamid Karzai: President of Afghanistan, ENCYCLOPEDIA BRITANNICA (Dec. 20, 2021), available at https://www.britannica.com/biography/Hamid-Karzai.
124) Julian Borger, Bonn Conference Could Mark Formal Start of Afghan Peace Process, THE GUARDIAN (Jun. 20, 2011), available at https://www.theguardian.com/world/julian-borger-global-security-blog/2011/jun/20/afghanistan-taliban-talks-bonn.
125) Scott Baldauf, & Owais Tohid, Taliban Appears to Be Regrouped and Well Funded, THE CHRISTIAN SCIENCE MONITOR (May 8, 2003), available at http://www.csmonitor.com/2003/0508/p01s02-wosc.html.
126) Pamela Constable, U.S. Troops Fired at Mob After Kabul Accident, THE SPOKESMAN-REVIEW (Jun. 6, 2006), available at https://www.spokesman.com/stories/2006/jun/01/us-troops-fired-at-mob-after-kabul-accident/.
127) Saeed Ali Achakzai, Taliban Reject Afghan President's Peace Talk Offer, REUTERS (Sep. 30, 2007), available at https://www.reuters.com/article/us-afghan-talks-idUSISL26606720070930.
128) Gareth Porter, US Silent on Taliban's al-Qaeda Offer, SOUTH ASIA (Dec. 17, 2009), available at https://web.archive.org/web/20091219213931/http://www.atimes.com/atimes/South_Asia/KL17Df02.html.

129) Olivier Laurent, When War Is Just Another Day in Afghanistan, TIME (Jul. 8, 2016), available at https://time.com/4402071/afghanistan-war-everyday/.
130) Ryan Browne, Carter visits Afghanistan as Obama Plans Handoff of 15-Year War, CABLE NEWS NETWORK (CNN) (Dec. 9, 2016), available at https://edition.cnn.com/2016/12/09/politics/ash-carter-afghanistan-visit/index.html.
131) James Griffiths, Trump Calls Out Pakistan, India as He Pledges to 'Fight to Win' in Afghanistan, CABLE NEWS NETWORK (CNN) (Aug. 24, 2017), available at https://edition.cnn.com/2017/08/21/politics/trump-afghanistan-pakistan-india/index.html.
132) James Rothwell, Mohammad Zubair Khan, & Bilal Sarwary, Taliban Holds 'Informal' Talks with Afghanistan, THE TELEGRAPH (Oct. 18, 2016), available at https://www.telegraph.co.uk/news/2016/10/18/taliban-holds-informal-peace-talks-with-afghanistan/.
133) Shereena Qazi, Afghanistan's Taliban, US Sign Agreement Aimed at Ending War, AL JAZEERA (Feb. 29, 2020), available at https://www.aljazeera.com/news/2020/2/29/afghanistans-taliban-us-sign-agreement-aimed-at-ending-war.
134) Hamid Shalizi, Abdul Qadir Sediqi, Rupam Jain, Taliban Step Up Attacks on Afghan Forces Since Signing U.S. Deal: Data, REUTERS (May 1, 2020), available at https://www.reuters.com/article/us-health-coronavirus-afghanistan-taliba/taliban-step-up-attacks-on-afghan-forces-since-signing-u-s-deal-data-idUSKBN22D5S7.
135) Bill Roggio, Taliban Squeezes Afghan Government by Seizing Key Border Towns, FDD'S LONG WAR JOURNAL (Jul. 9, 2021), available at https://www.longwarjournal.org/archives/2021/07/taliban-squeezes-afghan-government-by-seizing-key-border-towns.php.
136) Ava Batrway, Afghan President Latest Leader on the Run to Turn Up in UAE, ASSOCIATED PRESS NEWS (Aug. 19, 2021), available at https://apnews.com/article/europe-middle-east-39610b0102a926c1a573da3d6feb0eea.
137) Emma Graham-Harrison, 'Panjshir Stands Strong': Afghanistan's Last Holdout Against the Taliban, THE GUARDIAN (Aug. 18, 2021), available at https://www.theguardian.com/world/2021/aug/18/panjshir-stands-strong-afghanistans-last-holdout-against-the-taliban.
138) David Zucchino, The U.S. War in Afghanistan: How It Started, and How It Ended, THE NEW YORK TIMES (Oct. 7, 2021), available at https://www.nytimes.com/article/afghanistan-war-us.html.
139) John McCormack, Why Did the United States Abandon Bagram Airfield?, NATIONAL REVIEW (Aug. 18, 2021), available at https://www.nationalreview.com/2021/08/why-did-the-united-states-abandon-bagram-airfield/.
140) Barbara Sprunt, There's A Bipartisan Backlash To How Biden Handled The Withdrawal From Afghanistan, NATIONAL PUBLIC RADIO (Aug. 17, 2021), available at https://www.npr.org/2021/08/16/1028081817/congressional-reaction-to-bidens-afghanistan-withdrawal-has-been-scathing.
141) Zolan Kanno-Youngs, & Annie Karni, Series of U.S. Actions Left Afghan Allies Frantic, Stranded and Eager to Get Out, THE NEW YORK TIMES (Aug. 29, 2021), available at https://www.nytimes.com/2021/08/18/us/politics/afghanistan-refugees.html.
142) Juliegrace Brufke, supra, note 122.
143) Associated Press, EXPLAINER: What Happened to the Afghanistan Evacuation?, U.S. NEWS AND WORLD REPORT (Nov. 26, 2021), available at https://www.usnews.com/news/politics/articles/2021-11-26/explainer-what-happened-to-the-afghanistan-evacuation.
144) Glenn Kessler, No, the Taliban Did Not Seize $85 Billion of U.S. Weapons, THE WASHINGTON POST (Aug. 31, 2021), available at https://www.washingtonpost.com/politics/2021/08/31/no-taliban-did-not-seize-83-billion-us-weapons/.
145) SIGAR Staff, Section 2 Reconstruction Update, SPECIAL INSPECTOR GENERAL FOR AFGHANISTAN RECONSTRUCTION 29 (Jul. 30, 2021), available at https://www.sigar.mil/pdf/quarterlyreports/2021-07-30qr-section2-funding.pdf#Page=9.
146) Glenn Kessler, supra, note 207.
147) Zolan Kanno-Youngs, & Annie Karni, supra, note 203.
148) Converstation Staff, What's Next for Afghanistan? Two Experts Make Predictions, THE CONVERSATION (Nov. 30, 2021), available at https://theconversation.com/whats-next-for-afghanistan-two-experts-make-predictions-170684.
149) Colin Clarke, & Jonathan Schroden, Brutally Ineffective: How the Taliban Are Failing in Their New Role as Counter-Insurgents, WAR ON THE ROCKS (Nov. 19, 2021), available at https://warontherocks.com/2021/11/brutally-ineffective-how-the-taliban-are-failing-in-their-new-role-as-counter-insurgents/.
150) Boy Scout Oath, Law, Motto and Slogan and the Outdoor Code, US SCOUTING SERVICE PROJECT (n.d.), available at http://usscouts.org/advance/ScoutsBSA/oathlaw.asp. The Boy Scout web site contains the changes made to the principles of Scouting after January 01, 2019.

151) See generally, Adequate Prepardedness, MERRIAM-WEBSTER DICTIONARY (n.d.), available at https://www.merriam-webster.com/dictionary/preparedness.

152) See generally, Adequate Prepardedness, THE LAW DICTIONARY FEATURING BLACK'S LAW DICTIONARY (n.d.), available at https://thelawdictionary.org/adequate-preparation/.

153) The Cadmus Group LLC, Cybersecurity Prepardedness Evaluation Tool, NATIONAL ASSOCIATION OF REGULATORY UNITITY COMMISSIONERS (Jun. 2019), available at https://pubs.naruc.org/pub/3B93F1D2-BF62-E6BB-5107-E1A030CF09A0.

154) 'State of Surveillance' with Edward Snowden and Shane Smith (VICE on HBO: Season 4, Episode 13), YOUTUBE.COM (January 08, 2016), available at https://www.youtube.com/watch?v=ucRWyGKBVzo. Dodge v. Ford Motor Company, 204 Mich. 459 (1919).