STUDENT STUDY GUIDE

UNCLASSIFIED CONTROLLED TRAINING MATERIAL

HQ AFSPC/A3/6T 29 July 2019

Cyber Operations

Advanced Training

HQ AFSPC/A3/6T 29 Jul 2019

Table of Contents

List of Figures

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

HQ AFSPC/A3/6T 29 Jul 2019

Cyber Operations

1. Given associated reference materials and this lecture, identify potential vulnerabilities and threats to your weapon system with at least 80% accuracy

Samples of Behavior:

1. Given associated reference materials and this lecture, identify basic facts and terms pertaining to Cyber Operations with at least 80% accuracy
2. Given associated reference materials and this lecture, summarize the United States approach to Cyber Operations with at least 80% accuracy
3. Given associated reference materials and this lecture, describe the United States adversaries approach to Cyber Operations with at least 80% accuracy

Main Points:

1. Introduction to Cyber Operations
2. US approach to Cyber Operations
3. Adversary approach to Cyber Operations

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

HQ AFSPC/A3/6T 29 Jul 2019

Introduction to Cyber Operations

This lesson will provide an introduction to Cyber Operations (CO) and exposure to some of the threats that exist in today's technology-dependent environment. To understand Cyber Operations, we must first understand our own approach to CO. Joint Publication 3-12(R) provides direction to our joint forces, with regards to the use of cyberspace. It defines CO as "the employment of cyberspace capabilities when the primary purpose is to achieve objectives in or through cyberspace". Simply put, it is the use of cyberspace as a means to achieve our strategic objectives. CO play a key role in military operations due to its far-reaching impact.

What is Cyberspace

We often think of cyberspace simply as the internet most of us use on a daily basis. Although this is correct to some degree, the internet is just one of several components that make up cyberspace. According Joint Publication 3-12 (JP 3-12), "cyberspace is the global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers". What does this tell us? It tells us that although cyberspace is not a physical domain, it is supported by an enormous hardware and software infrastructure, and exists in all four of the physical domains (land, sea, air and space). We must think of cyberspace as much more than just the internet. Figure 1 provides a visual representation of the cyberspace domain.

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

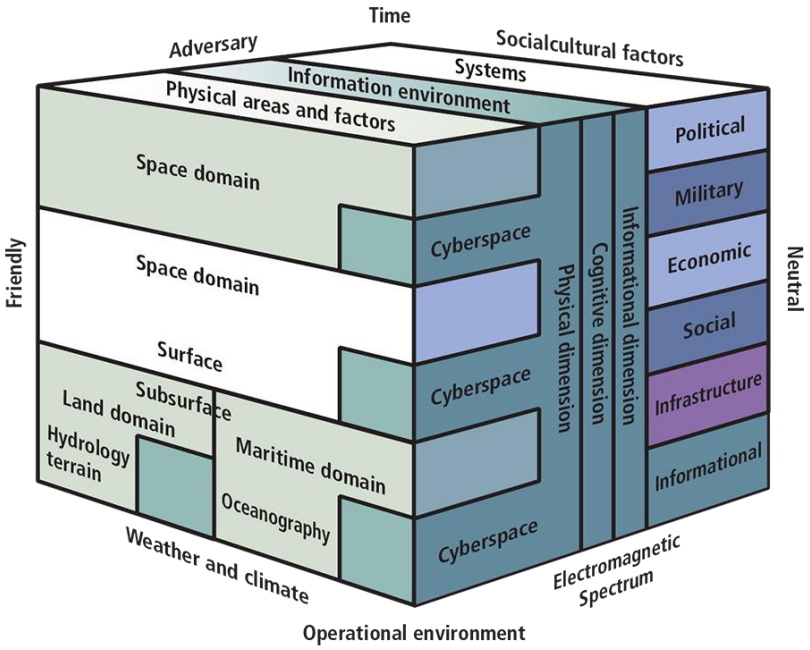


Figure 1: The Cyber Domain

Why is Cyberspace Important

Cyberspace is extremely important to the joint force and joint operations. JP 3-12 states "developments in cyberspace provide the means for the US military, its allies, and partner nations to gain and maintain a strategic, continuing advantage in the Operational Environment (OE), and can be leveraged to ensure the nation's economic and physical security". Cyberspace supports every aspect of military operations. Operations conducted in this domain have far reaching impact. On the other hand, our reliance on cyberspace presents some significant challenges. According to JP 3-12, "the prosperity and security of our nation have been significantly enhanced by our use of cyberspace, yet these same developments have led to increased vulnerabilities and a critical dependence on cyberspace, for the US in general and the joint force in particular". This is because "access to the internet provides adversaries the capability to compromise the integrity of US critical infrastructures in direct and indirect ways".

Layers of Cyberspace

JP 3-12 guidance views cyberspace in terms of three layers: the physical network layer, the logical network layer and the cyber-persona layer. Figure 2 provides a visual representation of the three cyberspace layers discussed in this lesson.

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

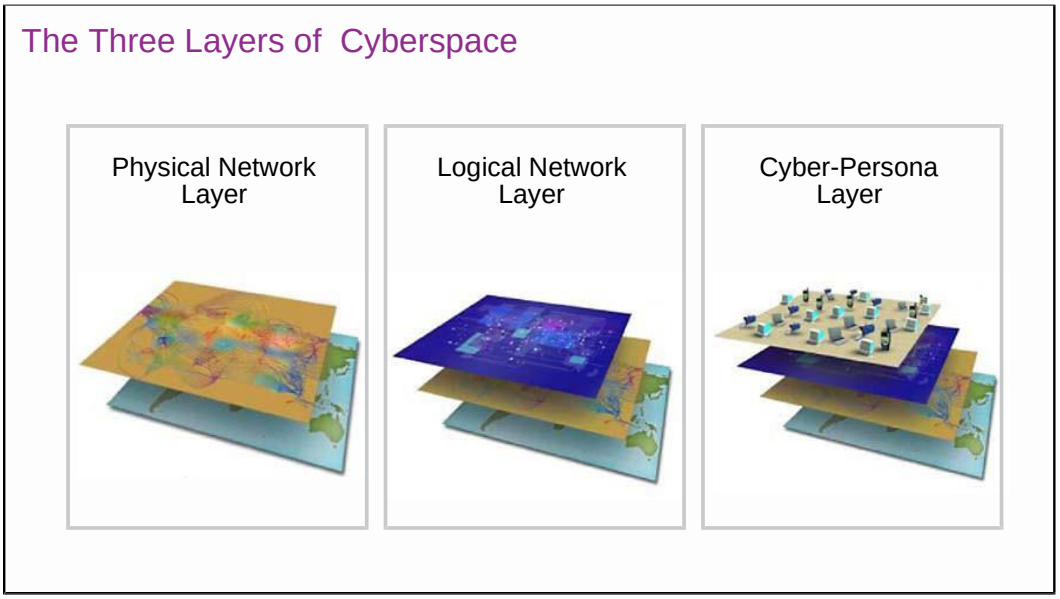


Figure 2: The Three Layers of Cyberspace

The **physical network** layer of cyberspace is comprised of a geographic component and physical network component. The geographic component is a physical location in which the network component operates; the four physical domains (land, sea, air and space). The physical network component consists of the actual hardware, software and infrastructure that make up the network. It is the equipment that allows data to be transported from one place to another.

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

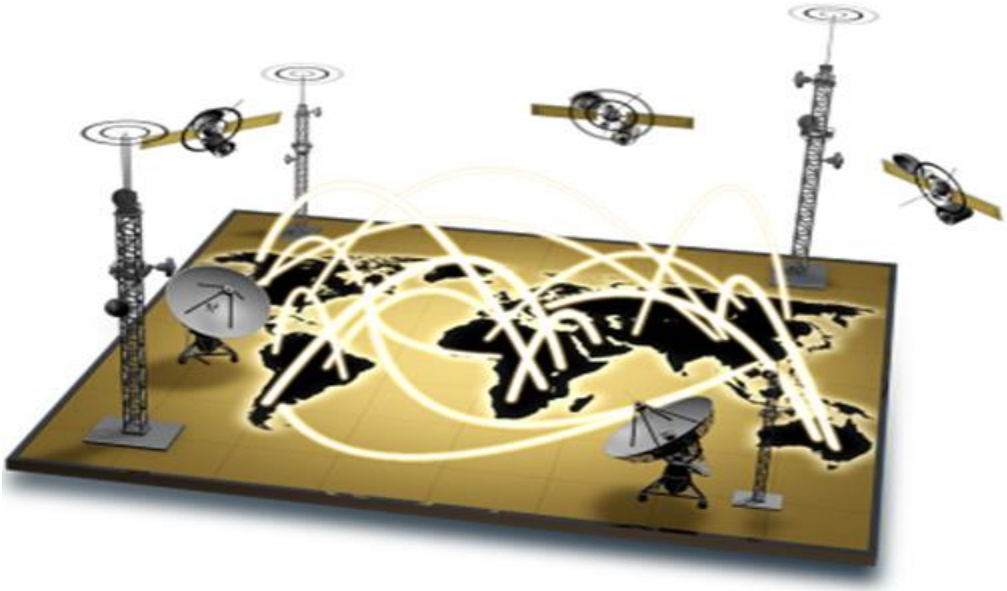


Figure 3: The Physical Network Layer

The **logical network** layer encompasses the digital relationships or associations that exist on a network. For example, the web address assigned to a website, connects the site and its content to a unique identifier. Even though this content may be distributed across multiple servers in multiple physical locations, the data may be accessed and displayed on a single web document by entering the assigned web address. The Air Force Portal is a perfect example.

Figure 4: The Logical Network Layer

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

The **cyber-persona** layer is comprised of the personnel operating the terminals or workstations connected to the network. A cyber-persona is the digital representation of a user on the network. Use of a persona is not restricted to a single user. Multiple users may utilize the same cyber-persona. For example, a common user account utilized by RADAR crewmembers; the profile for this account is not unique to any single user. Compare this common user profile to your profile on a social media site. Your social media profile is a digital representation of you. Also note that this digital identity may be real or fake. A hostile actor will most likely utilize a fake persona.

Figure 5: The Cyber-Persona Layer

US approach to Cyber Operations

Cyber Operations Terminology

To gain an understanding of Cyber Operations, we must first become familiar with some of the terminology. Joint CO are broken down into three categories; Offensive Cyber Operations (OCO), Defensive Cyber Operations (DCO) and Department of Defense information network (DODIN) operations; each has a very specific purpose. Understanding this terminology is important because we can safely assume our adversaries are conducting similar types of operations in addition to building and maintaining network infrastructure in support of their objectives. They may use different terminology, but the concept is the same.

Offensive Cyber Operations: According to JP 3-12, "OCO are CO intended to project power by the application of force in and through cyberspace. OCO will be authorized like offensive operations in the physical domains, via an execute order (EXORD). OCO requires deconfliction in accordance with current policies". Just as our joint force executes CO to achieve specific objectives or lay the groundwork for an operation, it is not unreasonable to expect our

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

adversaries to execute their own version of OCO in an attempt to "level the playing field". For this reason, vigilance is crucial, especially when conducting day-to-day operations. Cyber-attacks will come without warning (and in ways we may not have anticipated), so we must always be prepared to act. However, we cannot respond to an event that we do not know is taking place. Knowing the ins and outs of your weapon system will put you in the best position to detect when it is not functioning as it should and take the appropriate action. Having in-depth knowledge of how the RADAR system functions is key.

Defensive Cyber Operations (DCO): DCO are the CO we execute to defend DoD cyberspace assets and capabilities. They include active and passive defense operations, and afford us the ability to utilize our capabilities in this domain. DCO is critical to the protection of our data, cyberspace networks and the critical systems connected to these networks. According to JP 3-12, "DCO responds to unauthorized activity or alerts/threat information against the DODIN, and leverages intelligence, counterintelligence (CI), law enforcement (LE), and other military capabilities as required. DCO includes outmaneuvering adversaries taking or about to take offensive actions against defended networks, or otherwise responding to internal and external cyberspace threats". It is important to note that cyberspace threats do not always come from external sources.

Department of Defense information networks (DODIN): The DODIN are a set of globally interconnected information capabilities used to collect, process, disseminate and manage classified and unclassified data, making it readily available to joint users. Joint Publication 6-0 (JP 6-0) provides the following description: "The DODIN consists of all networks and information systems owned or leased by the DoD. This includes common enterprise service networks (classified and unclassified), intelligence networks operated by DoD components of the intelligence community (IC), closed mission system and battlefield networks, and other special purpose networks (e.g., "edu" domains operated by the Service academies). When properly secured, operated, and defended, the DODIN collects, processes, stores, manages, and disseminates information on demand to the joint force, policy makers, and support personnel. DODIN operations are the means by which DoD designs, builds, configures, secures, operates, maintains, and sustains communications and networks in support of military operations. DoD shares cyberspace with enemies and adversaries seeking to exploit our weaknesses on a daily basis. US joint forces, mission partners, and first responders require communications that are not only secure, but also flexible enough to meet the ever-changing needs of joint and multinational operations". Put simply, the DODIN is a critical cyberspace asset.

Computer Network Exploitation (CNE): CNE can be thought of as the process of intelligence gathering within the cyberspace domain. Computer systems are targeted for the collection of information. This is done through the use of computer networks. Techopedia.com states, "CNE is primarily used within military institutes and organizations. It is a type of cybersecurity

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

operation and can be considered equivalent to the jobs/processes of real-world spies or agents. It consists of techniques and processes that utilize computers or computer networks to penetrate targeted systems and networks." CNE is an ever-existing threat to our military operations, in addition to our national security. To mitigate this threat, we must ensure established security procedures are followed at all times, but especially while executing the day-to-day mission. Protecting sensitive data is one of our highest security priorities.

Computer Network Attack (CNA): A CNA is an offensive operation executed through the use of computer networks. The objective is to disrupt, deny, degrade, or destroy the information stored on computers and networks, or the actual computers and networks themselves. This task may be as simple as introducing malicious code onto a network, or as complex as defeating the security architecture, in an attempt to access sensitive information. CNA provides our adversaries with relatively low-cost options that can be utilized to target our critical information systems and networks. It is also important to note, a CNA is not limited to terrestrial networks. Space-based cyberspace components are also at risk.

- **Purposes/intent of CNA:** The purpose of a CNA is to achieve offensive strategic objectives through the use of computers and computer networks. The existing and ever-increasing global dependence on the cyberspace domain presents our joint force with a host of opportunities to affect the battlespace, without the limitation of physical boundaries. At the same time, it also presents our adversaries with a host of opportunities to do the same.

- **Deny.** The goal of "deny" is to prevent the adversary or target of an operation from being able to utilize their cyberspace capabilities (especially in an offensive manner). This inherently gives us the advantage of dominance within the domain and affords us the freedom to employ friendly capabilities while preventing the enemy from deploying its own. With this in mind, we must also be aware that our adversaries will most likely target friendly systems with deny operations in an attempt to gain the advantage while pursuing their mission objectives.

- **Degrade.** The goal of this technique is to reduce an adversary's cyberspace capability and the ability to accomplish their mission. If critical equipment is prevented from performing at its full potential it puts the adversary at a disadvantage. For example, if a network system responsible for disseminating time-sensitive data is slowed down it can have a direct impact on operational troops who depend on that data. The goal is not to prevent use of the equipment but to reduce its effectiveness.

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

- **Disrupt.** The goal of this technique is to temporarily interfere with the normal operation of an adversary's cyberspace assets. This is done through the employment of one or more of the other CNA techniques and conducted for a predetermined period of time.

- **Destroy.** The goal of this technique is to cause irreparable damage to an adversary's asset. This, in-turn, prevents employment of the asset on a permanent basis. The asset could be something as simple as critical data stored on an information system or critical infrastructure connected to the network.

- **Manipulate.** The goal of this technique is to control or change the adversary's data, their information systems, and/or networks, in a manner that best supports our objectives. We've all heard the term "information is power". If we are in a position to control the information that an adversary depends on, it will give us a significant advantage.

Brief History and Details about Air Force Cyber Warfare

Please read the handout "Air Force Cyber Warfare".

Adversary Approach to Cyber Operations

Cyber Security

Cyber warfare and the future of cyber security

Cyber warfare was a staple of movies like Tron, Hackers, or more recently, Mr. Robot.

In 2019, though, cyber warfare is no longer science fiction. Nation-states are increasingly seeing the cyber realm as an important military theater and deploying considerable resources to develop new types of attacks and ways to defend against them.

This is partly why there has been so much talk about cyber security in recent years. The techniques that companies, nation-states, and individuals are deploying to keep themselves safe are growing more sophisticated year after year. Cyber security is no longer for only multinationals and highly paid consultants; every day individuals are taking steps to avoid becoming a victim of cyber warfare.

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

Cyber warfare attacks are generally targeted at critical infrastructures such as power grids, nuclear enrichment facilities, and missile launch systems. Most of them rely on compromising civilian computers and other devices. This is because many attacks rely on recruiting consumer devices into botnets or simply using your devices as a way to infect military and corporate networks with malware. That means that everyone is exposed to the growing threats of cyber weapons, and everyone should take cyber security seriously. You might think that you are a long way from the frontline of inter-state warfare, but you are not. Today, your devices are a critical part of the battlefield.

What is cyber warfare

Cyber warfare is, essentially, warfare between states, albeit conducted in the cyber realm. It consists of states (and state-sponsored agencies) launching cyber-attacks against each other. The objectives of launching these attacks vary. Sometimes the motive is to steal corporate or state secrets. Sometimes an attack aims to disrupt critical infrastructure or merely infect the software behind this infrastructure and lay silent until it is needed. Some attacks even seek to influence elections by directly hacking voting software or distributing propaganda among crucial voters.

Even if two states are not actively at war, they will often launch cyber-attacks against each other. These attacks are cheap and mostly undetectable if done correctly. This makes cyber warfare a very attractive tool for states that can't risk the consequences of more conventional forms of attack. Cyber warfare attacks can be launched covertly and there is no internationally agreed upon framework for assigning blame or applying sanctions for cyber-attacks. Because of this states like Russia and Iran, and sometimes even the United States, launch cyber-attacks on a fairly regular basis.

Types of cyber-attack

Though concern over cyber warfare conflicts between states is what we focus on working in the DoD, many of the weapons used in cyber warfare are directed at civilians. In fact, many of these attacks rely on people like you and me practicing poor cybersecurity and make use of popular and widespread hacking techniques. Let's take a look at a few of these.

Man in the middle attacks

A common attack vector is to stage a man in the middle attack to gain access to key networks or information and then use the stolen data to launch further attacks. A man in the middle attack is a type of cyber-attack where a hacker intercepts the data passing between you and a website, app, or server. They can then read, steal, or even alter this data. In this way, you think you are

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

communicating with a legitimate and secure service but, in fact, you are sending critical information to an attacker.

Phishing

Phishing has been around as long as the internet but is more widespread than ever. Most phishing attacks are designed to get access to your banking details but phishing is also commonly used in cyber warfare. Phishing emails are an effective way of infecting a target with malware (discussed below). Once a machine, like your home computer, is infected an attacker can use your computer to launch further attacks against military or governmental targets.

Malware

Many forms of cyber warfare also make use of malware. Infecting government or military computers with malware is often the goal of cyber warfare attacks. In order for this to happen, an attacker needs to infect as many computers as possible with malware in order to increase the chances that one of them will then infect the target system. That means your computer is a valuable asset in the ongoing cyber war. Without realizing it, your devices could be full of military-grade malware just waiting until you connect to a target network.

The future of cyber security

The scale of cyber warfare today means that there is an ongoing arms race. As new forms of attacks emerge, new countermeasures are developed, avoided, then the cycle repeats. There are three key pieces of technology that are likely to drive the development of cyber warfare in the coming decade.

1. **Machine Learning And AI -** Artificial Intelligence is already being deployed in a wide range of situations and it is likely that governments are already incorporating it into their cyber weapons.

2. **The Cloud -** Cloud storage represents both a risk and an asset when it comes to cyber warfare. On one hand, distributed storage can make critical information easier to steal because an attacker only needs to identify one weak machine in order to compromise a system. On the other hand, with the correct encryption, cloud storage can actually be more secure than physical drives.

3. **Blockchain -** Blockchain is also likely to revolutionize cyber warfare in the coming years by providing a secure way to share key information between multiple users. It promises

to protect data from the most common types of cyber-attack. On the other hand, it is unknown how long it will be before blockchain is compromised and no longer effective.

Adversary attack behavior[7]

We will discuss the three key aspects that can lead to an adversary's successful cyberattack; means, motive, and opportunity. By the end of the section you should be able to identify how these three aspects translate into the notions of probability of attempt and probability of success.

Opportunity, Motive, and Means for Cyber Attacks

Understanding the opportunity, motive, and means of an adversary is helpful in protecting your weapon system and/or devices from the potential of falling victim to an attack. An adversary may be faced with several potential attack options. The adversary must first determine which attack options are available (i.e., where the adversary has the opportunity to attack) and then determine which available attack option is most attractive (i.e., where the adversary has the motive to attack and the best potential opportunity for success). The success of an attack attempt is determined by the adversary's capability and if they have the means to defeat the target system's defense.

Opportunity: Attack Precondition

The attack precondition outlines the adversary's first step in regards to deciding whether they want to attempt an attack on a target system or not. This attack step requires the attacker to possess the minimum level of system access, system knowledge, and attack skill needed to attempt the attack as perceived by the adversary. The attack step precondition is a necessary, but not sufficient, condition for an adversary to attempt an attack.

Example #1: When the attack step consists of an adversary gaining corporate network access from the Internet through the company's Virtual Private Network (VPN), the attacker must possess Internet access and either knowledge of VPN account log-in information or VPN software exploit skill. An adversary who have that information may be enough to discourage an attack attempt.

Example #2: In layman's terms, this can equate to a thief watching your home and identifying the type of home security you have. The thief then determines whether they have the skill and tools necessary to disable your home alarm.

Motive: Probability of Attempt

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

The adversary possesses the motive to attack when he or she determines the opportunity for an attack exists. The probability of an adversary to attempt a specific attack includes an assumption the time required to execute the attack exists. The time period for an attack varies and may be as long as a decade depending on the skills required and overall objective of the attack. The probability of attempting a particular attack depends on the relative attractiveness of that attack. The adversary first considers all available attack options, including the option to attempt no attack (the "do-nothing" attack step). The adversary then rates the attractiveness of each option using his or her personal attack goals and available targets. Attack target preferences describe the relative importance of four attractiveness measures.

The four attractiveness measures are:

1. Cost to the adversary in attempting the attack
2. Payoff to the adversary for successfully executing the attack
3. Probability of successfully completing the attack, as perceived by the adversary
4. Probability of being detected by the system during or after attempting the attack

Different adversaries may have different attack preference weights. A well-funded nation-state may care little about the cost of an attack but may tolerate only very low probability of detection in the attacks it chooses to attempt. However, a resource-constrained lone hacker may try riskier attacks with a low probability of success and high probability of detection, but the cost to attempt must be low.

After the set of available attack options have been rated with respect to attractiveness to a particular adversary, the adversary chooses the appropriate type attack to attempt based on their resources and objectives. In certain circumstances, the "do-nothing" attack may be the most attractive option. Although the "do-nothing" attack has no payoff, it also has zero cost, no probability of detection, and no probability of failing. In fact, when the "do-nothing" attack is consistently the most attractive attack step option for adversaries, this is a sign of a strong system defense. This situation means that the available attack options are too costly, with too little payoff, too high a probability of detection, and too low a probability of success from the point of view of the attacker.

Means: Probability of Success

The probability of successfully executing the attack is based on the balance of the attack skill of the adversary versus the defensive strength of the system. The defeat of strong system defenses requires more advanced attack skills and, possibly, resources that may or may not be available to the adversary.

What to do about it

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

The first step is to follow your local cyber security procedures. Often times this includes some level of encrypting your files and email. While it might not seem like you have much power in comparison to the governments that want to compromise your security and privacy, you do. This is a simple way to reduce your exposure to cyber-attacks, whether these are deployed as part of cyber weapons or merely to make money for a hacker, is to encrypt all of the information you send and receive online.

Encryption is a powerful tool to protect your information and privacy because it means that even if someone manages to get hold of your data they won't be able to read it. There are many types of encryption and the technique is used across a wide variety of devices. Encryption stops anyone from being able to read the data you are sending, it protects you against many common forms of cyber-attack, including man in the middle attacks and Domain Name System (DNS) Spoofing. It also keeps you anonymous online, and therefore protects your privacy.

The ultimate form of encryption is to use end-to-end encryption for everything you do online. That might sound complicated, but it is not. By using a VPN you can make sure that every piece of information you send or receive online is encrypted. Most VPNs will also protect you against a wide array of online threats whether these arise as part of government cyber weapons or are merely the work of a lone hacker.

Profiles in cyber: Understanding the US's major adversaries in cyberspace[8]

This is a concise introduction and convenient reference to the distinct motives, narratives, strategies, capabilities and operations of each nation-state threat actor. For the full, unabridged, article go to: www.fifthdomain.com/home/2017/05/26/profiles-in-cyber-understanding-the-uss-major-adversaries-in-cybersapce/

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

HQ AFSPC/A3/6T 29 Jul 2019

Russia

You may not be interested in war, but war is interested in you. – Leon Trotsky

Cyber Strategy

In early 2013, Chief of the General Staff of the Russian Federation, Valery Gerasimov, published an article that laid out a "new-type" warfare. Dubbed the Gerasimov Doctrine by some experts, it's alternately known by terms such as next-generation warfare, nonlinear warfare and full-spectrum warfare, among others. U.S. academic literature refers to it as hybrid warfare, while the U.S. military refers to it as hybrid threats.

A primary goal of Russia's hybrid warfare and cyber strategy is to undermine Western democratic ideals and institutions, including within the U.S., but also among U.S. allies such as the European Union and international organizations such as NATO. Russia calls the peacetime application of these subversive techniques "active measures," which are carried out by the Russian military and security services.

Gerasimov was as keenly aware of "new-type" warfare for offensive purposes as he needed to guard Russia against it. Almost a year to the day after Gerasimov's publication, the threat he had warned of arrived on Russia's doorstep in early 2014 via the Euromaidan Revolution in Ukraine. Recognizing its domestic vulnerabilities, Russia censors its internet, controls its media and is believed to employ widespread surveillance on its citizens.

Cyber Capability

Russia is usually cited as the U.S.'s foremost foe in cyberspace. While the Chinese are believed to rival Russia's level of technical, operational and informational capability, Russia has historically shown less reluctance than China to use cyber for aggressive tactics, including cyberwarfare against regional neighbors.

In addition, Russia is believed to employ a broader range of cyber tactics than China in service of its strategic goals. For instance, Russia uses cybercriminal proxies and online information warfare front groups (e.g., fake news, troll factories, etc.) in ways that China does not.

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

Russia's sophisticated technical capabilities, diverse tactics and willingness to operationalize offensive cyber in furtherance of its sometimes controversial national interests all factor into Russia's frequent ranking as the U.S.'s top cyber adversary.

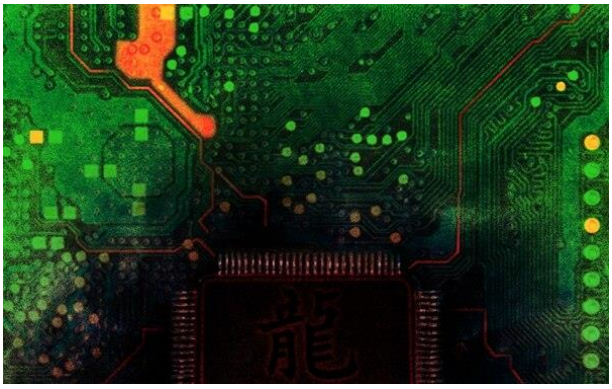
Cyber Operations

Cyber operations have proven a new, highly effective means and medium for hybrid warfare, which Russia displayed in cyberattacks against Estonia in 2007, the country of Georgia in 2008 and Ukraine from 2014 to present. In addition, cyber has proven effective in conducting what a pre-cyber KGB historically called active measures. Retired KGB Maj. Gen. Oleg Kalugin summarized active measures as techniques for subversion, with the goal to "weaken the West."

Russian cyber operations often blend elements of intelligence gathering and active measures. A prime example is the 2016 U.S. presidential election, in which Russia used cyber-espionage hacking to gather intelligence from political targets and then used the stolen information in cyber-enabled active measures (e.g., disinformation, front groups, etc.) to subvert the U.S. political process.

Russia also makes extensive use of proxies to carry out cyber operations. The exact connection between these proxies and the government is often ambiguous. Perhaps more than any other country, Russia employs these cybercriminals. For years, cybercriminals, acting as cyber proxies affiliated with the Russian Business Network conducted cyberattacks against U.S. and other Western institutions from inside Russia with impunity. Journalist Brian Krebs has reported that convicted hackers in Russia can shorten jail sentences by agreeing to hack for the government.

China



All war is deception. Be extremely subtle, even to the point of formlessness. Be extremely mysterious, even to the point of soundlessness. Thereby you can be the director of the opponent's fate. – Sun Tzu

Cyber Strategy

Like other nations, China watched the impressive show of U.S. military dominance in Operation Desert Storm and realized it could not defeat the U.S. in conventional warfare. In 1999, two colonels in the People’s Liberation

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

Army (PLA) wrote the book *Unrestricted Warfare*, which sets out a strategy to use nonmilitary means to achieve geostrategic and military goals.

"When we suddenly realize that all these non-war actions may be the new factors constituting future warfare, we have to come up with a new name for this new form of war," the authors wrote. *"Warfare which transcends all boundaries and limits, in short: unrestricted warfare."* For the Chinese, these include psychological warfare, media warfare and legal warfare.

Two strategic concepts, in particular, have influenced China's thinking on and use of cyber, specifically. The first is the concept of "informationization," and the second is "active defense."

In recent decades, Chinese military and strategic writers have increasingly referred to the concept of "informationized warfare," which focuses on "information dominance" (zhi xinxi quan) via cyber, electronic and space operations. Experts say informationization is roughly equivalent to the U.S. concept of network-centric warfare. In 2004, at the onset of China's ambitious modernization of its military, then-President Hu Jintao cited the need to fight "informationized local wars," a concept echoed word-for-word by PLA leadership in recent national military strategic guidelines, according to the U.S. Department of Defense.

The second strategic principle that has influenced China's thinking on cyber is "active defense," which the U.S. Defense Department explains as follows:

China characterizes its military strategy as one of “active defense,” a concept it describes as strategically defensive but operationally proactive in orientation. It is rooted in a commitment not to attack, but to respond aggressively once an adversary decides to attack – a defense that counterattacks in order to disrupt an adversary’s preparations or offensive rather than a defense that reacts passively. The PLA interprets active defense to include mandates for both de-escalation and seizing the initiative.

China's cyber strategy also emphasizes the principles of sovereignty, non-interference and states' rights to control online content, the last illustrated most notably by the Great Firewall of China.

Cyber Capability

Like Russia, China has developed formidable cyber capabilities over the past two decades. Unlike Russia, China is not known to have used its capabilities in cyberwarfare or to allow cybercriminal proxies to act on the state's behalf of its goals.

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

China has instead focused on extensive, multi-year cyber espionage against the West and the U.S., in particular. China's cyber espionage operations include political and military intelligence gathering, which is viewed as a reality in traditional statecraft, but also more controversially in economic espionage. The scale, scope and duration of China's economic espionage has created friction in U.S.-China relations in recent years.

In terms of technical and operational skill, China most likely rivals Russia.

Cyber Operations

China's cyber operations are well resourced and capable of developing and using an array of advanced Tactics, Techniques and Procedures (TTPs). Today, the PLA continues a significant, ongoing, multi-decade initiative to modernize, reorganize and ultimately optimize its operations to the "informationized" environment, in which network-centric warfare is the focus. The publication China National Defense News noted that PLA leaders view networks as an Assassin's Mace (Shashou Jian), an inferior weapon that can deal the decisive blow to a superior adversary.

To date, China has engaged primarily in two types of cyber operation:

1. Cyber espionage
2. Gaining and maintaining persistent access to critical infrastructure, such as industrial control systems (ICS) and Supervisory Control And Data Acquisition (SCADA) systems

The results of China's commercial cyber espionage are remarkable: China is estimated to steal $300 billion worth of intellectual property from U.S. companies annually, resulting in what Gen. Keith Alexander (retired), former director the NSA, has called "*the greatest transfer of wealth in history*."

Given the advantages that cyber affords, including low relative cost of operations, anonymity, geographic reach and plausible deniability, China will not likely stop its massive, ongoing cyber espionage operations until some factor changes the strategic equation.

Persistent access to adversaries' critical infrastructure positions China to inflict a costly cyber counterattack should military circumstances require it. This capability fits within China's broader military strategy, notably the concept of active defense.

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

Iran

In the cyberwar between Iran and America, the defining issue is culture. The world in the 21st century is a world of thoughts and ideas, and not of hardware… Nowadays, America is the symbol of the evil person and the Islamic Republic is the symbol of the divine person. There is no common ground for these two. One of these two must be victorious over the other. – Islamic Revolutionary Guards Corps Brigadier General Second Class Behrouz Esbati, Operations Commander at Iran's Cyber Headquarters

Cyber Strategy

Since the 2010 discovery of the Stuxnet cyber-attack on its nuclear enrichment program, Iran has sought to formulate a cyber strategy. In recent years, Iran has continued to enhance its cyber capabilities, and cyber may be its weapon of choice in the current strategic environment.

Iran's interest in cyber is three-fold:

1. It fits Iran's strategic culture, particularly "a preference for ambiguity, standoff and indirection when conducting high-risk activities;"
2. The absence of international cyber operations norms, which provides Iran with "margin to maneuver;"
3. The opportunity to shape cyber norms, in favor of its behaviors

As with every other major U.S. adversary, Iran remains watchful and wary of its domestic vulnerabilities, particularly to information operations. Iran has viewed cyber as a key defensive tool since, particularly via internet censorship and domestic surveillance.

Cyber Capability

Iran's technical and operational capabilities do not match Russia's or China's, and it's possible that North Korea currently surpasses Iran, in terms of TTPs. But experts warn that Iran is an emergent cyber power that should neither be ignored nor underestimated.

Most threat intelligence and cyber-attack forensics published to date suggests Iran and its cyber proxies still rely on purchasing, stealing or repurposing cyber TTPs developed by others, rather than developing their own. This was most recently illustrated in a report wherein cybersecurity

researchers at TrapX observed Iran using the BlackEnergy malware to attack a U.S. defense contractor. Prior cybersecurity research showed the Iran-linked Shamoon group repurposed TTPs used against Iran, including the Flame malware and components of Stuxnet.

Cyber Operations

The discovery of the Stuxnet cyberattack in 2010 changed the way Iran thinks about cyber. Compared to Russia, China and even North Korea, Iran is most likely lagging in developing and operationalizing its own TTPs. The capabilities gap is narrowing quickly due to four factors.

1. The intellectual and innovative abilities of Iran's historically technically gifted population.
2. The ease with which it can purchase, steal or repurpose existing TTPs.
3. A cash infusion and recently lifted economic sanctions in the wake of the nuclear agreement reached with the U.S. and other Western countries.
4. The scientific and technological cooperation agreement signed with North Korea in 2012.

Similar cyber TTPs have been observed in recent cyberattacks believed to be carried out by Iran and North Korea.

Although Iran is known to engage in extensive domestic surveillance, not much has been published on the extent of its foreign cyber espionage operations. It is unclear whether the lack of knowledge equates with a lack of capability or a lack of detection. To date, cybersecurity research suggests Iran has been more focused on carrying out destructive or disruptive cyberattacks. The most well-known destructive cyberattack was carried out against Saudi Aramco in 2012. The Aramco attack destroyed approximately 35,000 computers using a wiper program.

Research and reports suggest Iran is also developing its capabilities to attack critical infrastructure, as evidenced by a 2013 cyberattack that allowed Iranian threat actors to temporarily take control of a small dam in New York State by compromising the dam's Industrial Control System (ICS). ICS systems are prevalent in critical infrastructure.

Cyber Posture

Iran's cyber posture is unpredictable and ranges from disruptive or destructive retaliatory cyberattacks to covert cyber espionage and reconnaissance activities. As illustrated by the Shamoon attacks, Iran's cyber operations are at times aggressive and indiscriminately destructive, although cyber proxies often carry out operations to provide plausible deniability. At

other times, Iran appears to lay low and engage in covert cyber espionage against international adversaries and surveillance against its domestic population.

North Korea

I have talked many times, but modern warfare is an electronic warfare. I can say that the victory and defeat of modern warfare depend on how we do electronic warfare.
– Kim Jong Il

Cyber Strategy

Former North Korean leader Kim Jong Il recognized the importance of cyber, information and electronic warfare as the Information Age dawned.

In 2013, South Korea's National Intelligence Service Director Nam Jae Joon testified that current leader Kim Jung Un allegedly said, "*Cyber warfare, along with nuclear weapons and missiles, is an all-purpose sword that guarantees our military's capability to strike relentlessly.*"

North Korea's cyber strategy fits within its traditional military strategy, which entails two primary goals, according to a Center for Strategic and International Studies report:

1. Disrupt opponents' conventional military operations.
2. Peacetime asymmetric methods that disrupt, destroy, exhaust or coerce adversaries, while remaining below the threshold to justify conventional military response.

Cyber Capability

North Korea is usually estimated to be less sophisticated than Russia or China. It's unclear how North Korea compares to Iran in terms of technical capability. North Korea's cyber operations are formally organized and integrated within its military.

Like Russia and Iran, North Korea is known to use cyber proxies, also known as a cyber-mercenaries or cyber-criminals. The most well-known is the hacking collective Lazarus Group, which has been linked to North Korea by multiple cybersecurity researchers. However, the exact nature of the connection between Lazarus Group and the North Korean military (if the two are distinct) remains unclear. Like Iran, North Korea has been known to use TTPs developed by

others. Cybersecurity researchers have also shown that Lazarus Group, and a subgroup dubbed Bluenoroff, consistently develop, rotate and use new TTPs to avoid detection.

North Korea is also believed to have more established cyber espionage capabilities than Iran presently has, but the exact scope and scale of the North's cyber espionage operations are difficult to estimate. In 2012, North Korea signed a scientific and technology cooperation agreement with Russia, China, Syria, Cuba and Iran, according to a 2014 report developed by Hewlett-Packard's security unit.

Cyber Operations

North Korea maintains active and formidable cyber operations. South Korea Defense Security Command Chief Cho Hyun Chun estimated North Korea had approximately 6,800 cyber warriors in 2016. If true, that number illustrates North Korea's significant investment in cyber, considering defector Jang Se Yul estimated the number to be 1,800 just three years ago.

North Korea's cyber operations are formally organized and integrated within the broader military structure. The Reconnaissance General Bureau (RGB), of which the infamous Bureau 121 is a part, is more active during peacetime. RGB is responsible for North Korea's non-cyber provocative acts, such as ballistic missile testing, as well as cyberattacks, including the 2014 Sony Pictures hack. RGB is also responsible for North Korea's cyber espionage operations.

The General Staff Department (GSD) oversees conventional military cyber operations and readiness. The GSD would provide the Korean People's Army cyber capabilities in the event of a conventional war, targeting adversaries' technological military systems such as command and control. In December 2016, North Korea hacked South Korea's command and control systems. The purpose of the cyberattack is unclear. Weeks later, the Korea Herald reported that South Korea's Defense Agency for Technology and Quality cited a Pentagon simulation that showed a full-fledged cyberattack from Pyongyang could "paralyze" U.S. Pacific Command.

Based on its philosophy of "quick war, quick end," North Korea is believed to engage in the Chinese equivalent of "active defense", whereby North Korean hackers gain and maintain persistent access to adversaries' critical infrastructure for quick-strike retaliation to a conventional military attack. It is unclear to what extent North Korea may have already infiltrated U.S. critical infrastructure. Even if North Korea does not maintain persistent access, it's likely capable of launching an effective cyberattack in short order.

Cyber Posture

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

The one adjective most often used to describe North Korea is *provocative*. The highly disruptive and destructive cyberattacks this decade, ranging from the Dark Seoul attack in 2013 to the Sony Pictures hack in 2014, were designed to get attention. Given its history and strategy, North Korea will likely continue to be a highly visible, extremely aggressive cyber provocateur, with a penchant for spectacularly disruptive and destructive cyberattacks.

State/non-state cyber-attacks[9]

In warfare, cyber or otherwise, nation states have the advantage of being on the proper legal and ethical side of things, and the potential advantage of having greater access to resources and materials. However, they have the distinct disadvantage of being bound by rules and morals, and are greatly restricted in their actions. Non-state actors take part in cyber warfare, but are not directly part of a nation state. Non-state actors can include script kiddies, scammers, hacktivists, blackhat hackers, criminal organizations, and other individuals or terrorist groups. Cyber-attacks in general cause disruption and confusion in day to day activities across the world, from the WannaCry attack in 2017, which hit hospitals and swept through hundreds of countries, to the 2015 hack that shut down Ukraine's power grid.

So what countries should we be most wary of in the cyber realm, and what attacks has these top hacking countries launched?

Top 10 of the world's largest cyberattacks[10]

Looking back over the years and what we see happening now is the same attack vectors being used that have led to breaches. Web applications and the human element of security remain the cornerstones when it comes to protecting your mission area against any weak spots, which cyber criminals are aware of and willing to exploit.

The number of cyber-attacks has grown steadily during the last few years. In 2016, 758 million malicious attacks occurred according to KasperskyLab, an attack launched every 40 seconds and there is no doubt that 2019 will break

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

the record. In 2017, ransomware was under the spotlight with the WannaCry and NotPetya attacks which temporarily paralyzed many large companies and organizations. The types of cyber-attacks are almost as numerous as the number of hackers. From individuals' personal information to confidential industrial product data, the field is vast and the consequences can be multiple: impersonation, banking data fraudulent use, blackmail, ransom demand, power cuts, etc. Often, it is the exploitation of system and network vulnerabilities that is responsible for cyber-attacks but these can often be avoided.

Below are a few examples of companies that have fallen victim and paid a high price for it. The ranking is presented in increasing order of impact based on number of victims. For the full, unabridged, article go to: https://outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks

10. Adobe was going through hell

Adobe announced in October 2013 the massive hacking of its Information Technology (IT) infrastructure. Personal information of 2.9 million accounts was stolen (logins, passwords, names, credit card numbers and expiration dates). Another file discovered on the internet later brought the number of accounts affected by the attack to 150 million (only 38 million active accounts). To access this information, the hackers took advantage of a security breach at the publisher, specifically related to security practices around passwords. The stolen passwords had been encrypted instead of being chopped as recommended. Fortunately, if this had led to banking data also being stolen, it was at least unusable because of a high-quality encryption by Adobe. The company was attacked not only for its customer information but also for its product data. The most worrying problem for Adobe was the theft of over 40GB of source code. For instance, the entire source code for the ColdFusion product was stolen as well as parts of the source codes for Acrobat Reader and Photoshop. If other attacks were to be feared, they did not ultimately take place.

9. Panic at Sony

In April 2011, Sony's PlayStation Network (PSN) was attacked. The multiplayer gaming service, online gaming purchasing and live content distribution of the Japanese brand contained the personal data of 77 million users which was leaked. Banking information of tens of thousands of players was also compromised. After the intrusion discovery, PSN, as well as Sony Online Entertainment and Qriocity, were closed for one month. To appease their users, Sony paid 15 million dollars in compensation plus a few million dollars in legal fees in addition to having to refund the people whose bank accounts had been illegally used. This cyber-attack could have been largely avoided. Hackers used a well-known network vulnerability that Sony chose to ignore. Data was unencrypted and could easily be hijacked thanks to a very simple Structured Query Language (SQL) injection. Unfortunately, in November 2014 a subsidiary, Sony Pictures

Entertainment, was attacked by malware and more precisely, by a computer worm. The "Guardians of Peace" stole 100 terabytes of data including large quantities of confidential information such as film scripts, compromising emails and personal data of 47,000 employees (names, addresses, emails, social insurance numbers, salaries etc. Business executive and producer Amy Pascal was ejected from her position because of the shocking content of her emails (judged insulting to then-President Barack Obama). In addition, the company cancelled the broadcast of several movies and paid the equivalent of 8 million dollars in compensation to its employees and former employees. The cyber-attack could have once again been avoided. Sony Pictures had carried out an audit of its security system a few months prior to the incident, and this audit had revealed serious failures in the infrastructure management, including a firewall and several hundred terminals (routers and servers) that were not managed by competent teams.

8. The South Korean nightmare

The South Koreans learned in January 2014 that data from 100 million credit cards had been stolen over the course of several years. In addition, 20 million bank accounts had also been hacked. For fear of having their bank accounts emptied, more than 2 million South Koreans had their credit cards blocked or replaced. Behind the theft was an employee of the Korea Credit Bureau (KCB), a solvency company. He stole personal information from customers of credit card companies when he worked for them as a consultant by simply copying the data to an external hard drive. He then resold the data to credit traders and telemarketing companies.

7. Target targeted

Target, the second-largest US discount retail chain, was the victim of a large-scale cyber-attack in December 2013. Data from 110 million customers was hijacked between November 27 and December 15 including banking data of 40 million customers and personal data (names, postal addresses, telephone numbers, and email addresses) of another 70 million customers. And it was not Target who discovered the attack. The American secret services had detected abnormal bank movements and warned the brand. According to several United States security services, the hacker group was located in Eastern Europe. It had installed malware in cash registers to read information from the credit card terminals. This technique is known as Random Access Memory (RAM) Scraping. Once the data had been hijacked, the attackers resold it on the black market. Target was ultimately required to pay over 18 million dollars as a settlement for state investigations into the attack.

6. Alteryx data leak exposes 123 million households

A marketing analytics firm left an unsecured database online that publicly exposed sensitive information for about 123 million U.S. households. The data included 248 fields of information

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

for each household, ranging from addresses and income to ethnicity and personal interests. Details included contact information, mortgage ownership, financial histories and whether a household contained a dog or cat enthusiast. Names were not included.

5. Equifax: a tricky crisis management

Equifax, an American credit company, revealed, six weeks after the initially identifying the attack, that it had suffered a cyber-attack over the course of a number of months. Detected in July of 2017, it contained the personal data (names, birthdates, social insurance numbers, driver license numbers) of 143 million American, Canadian and British customers as well as 200,000 credit card numbers. Complaints against the company as well as suspicions of insider trading were levied since the vulnerability of the open source web application Apache Struts used by the hackers was well known and several executives of the company sold stock just days before the security breach was made public.

4. Adult Friend Finder exposed

In 2015, the dating site was attacked for the first time. The information (pseudonyms, dates of birth, postal codes, Internet Protocol (IP) addresses, and sexual preferences) of 4 million accounts was made public on a forum only accessible on The Onion Router (Tor). Had it been recovered by malicious actors, the data could have been used for spam campaigns, identity theft or blackmail. However, no banking data had been hijacked. But the following year Adult Friend Finder faced a new attack, much more violent than the first one. This time it was not 4 million accounts pirated but more than 400 million. The stolen information was less sensitive but in total, 20 years of personal data was stolen. Attackers used a Local File Inclusion (LFI) breach, a technique that consists of introducing a local or remote file into an online resource. In addition, some former users had the unpleasant surprise to learn their personal information had not been deleted despite their account cancellations. This hacking record largely dethroned the Ashley Madison site cyber-attack.(In August 2015, the Ashley Madison extramarital dating site was hacked and personal data (names, email addresses, phones, sexual preferences) of more than 30 million users across more than 40 countries was harvested.

3. Marriott hotels: privacy of 500 million customers compromised

Information from up to 500 million guests at the Marriott-owned Starwood hotel group has been compromised, including banking data. The vulnerability had been open since 2014 and was first spotted September 2018. Even if, as Marriott says, the number of customers that suffered a breach of personal information is anywhere near 327 million, the implications are massive. Information accessed includes payment information, names, mailing addresses, phone numbers, email addresses, passport numbers, and even details about the Starwood Preferred Guest (SPG)

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

account, a high-end card launched by the American Express credit card issuer for regular travelers. "Marriott was first alerted to a potential breach in September 2018, it said, when an internal security tool found someone was trying to access its database. It then found that people seemed to have been in the database since 2014, and they had copied information apparently with a view to taking it." Marriott now faces a $123 million fine by United Kingdom (UK) authorities over this breach.

2. Theft of more than one billion passwords

In August 2014, the IT security company Hold Security revealed that Russian hackers had stolen 1.2 billion logins and passwords on 420,000 websites around the world. And this could potentially have allowed the group of hackers "CyberVor" to access 500 million email accounts. Hackers used programmed botnets to visit sites and perform vulnerability tests in order to exploit SQL injection vulnerabilities and access databases. While the attack is significant on account of its scale it has ultimately had no major consequences. According to the Federal Bureau of Investigation (FBI), the information has only been used in a large spam campaign on social networks (for instance) while the real intent of this hacking record remains a mystery for the organization.

1. Yahoo!: hackers favorite target?

In 2014, Yahoo! announced it had suffered a cyber-attack in 2014 that affected 500 million user accounts constituting the largest massive hacking of individual data directed against a single company. Names, dates of birth, telephone numbers and passwords were stolen. While the company assured users that banking data had not been affected it nonetheless recommended caution. Prior to this event, in 2012, the hacker “Peace” had sold 200 million usernames and passwords for $1900. Because bad things always come in threes in March, Yahoo! confessed to being hacked once again. This time "only" 32 million accounts were affected, but the cyber-attack relaunched the investigation of the 2014 hack, as the attackers used a tool stolen that year, allowing them to create malicious cookies and log in without passwords. A direct result of this is that the firm was bought by Verizon in 2017 for $ 4.5 million instead of the $ 4.8 million announced in 2016. Update (Dec 2018): Yahoo has now admitted that all of the 3 billion user accounts had been hacked in 2013. This cyber-attack is the most significant in Internet history.

Adversary approach to Cyber Operations Conclusion

While the previous cyber-attacks are impressive, many more are taking place every day in different business sectors or through different means. Recently, Home Box Office (HBO) lost 1.5 terabytes of data, including Television (TV) show episodes, scripts, manager emails and some Game of Thrones actors’ phone numbers. Dozens of US energy suppliers have also been

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

attacked and hackers can cut electricity anywhere in the United States at any time. How do we protect against cyber-attacks? Updating IT systems is the first step, but the best is to continuously detect vulnerabilities and fix them quickly to avoid attacks. The answers to many of the risks identified in this section are mostly unchanged and most of them, in theory, are simple. However, implementing the right solutions and especially maintaining their effectiveness heavily depends on the organization and training its personnel to be aware of illicit activity.

Summary

Throughout this lesson we have covered an introduction to Cyber Operations, and exposure to some of the threats that exist in today's technology-dependent environment. To understand Cyber Operations, we learned about the United States approach to Cyber Operations. Joint Publication 3-12(R) provides direction to our joint forces, with regards to the use of cyberspace. We also defined Cyber Operations as "the employment of cyberspace capabilities when the primary purpose is to achieve objectives in or through cyberspace".

Regarding Cyber Operations, you should now be familiar with terminology common to the cyber domain. CO are broken down into three categories; Offensive Cyber Operations (OCO), Defensive Cyber Operations (DCO) and Department of Defense information network (DODIN) operations; each has a very specific purpose. We briefly identified some of our adversaries, their motivations and capabilities. Finally, the top cyber-attacks around the world were identified in the hopes of showing you the targets of recent cyber-attacks and the potential vulnerabilities that may exist in our mission systems.

After reviewing the information in this lesson, you should be able to identify possible vulnerabilities in your mission system. Although the Air Force has an entire mission area dedicated to protecting mission systems from a cyber-attack, you should understand that each individual person has a responsibility, and the ability, to keep our networks safe on a daily basis. To ensure mission success, it is imperative that we all follow established security procedures. Additionally, continuing to learn about your weapon system and becoming an expert will better enable you to detect abnormal system behavior, which may indicate a cyber-attack.

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

HQ AFSPC/A3/6T 29 Jul 2019

Glossary of Terms

Active measures - a term for the actions of political warfare conducted by the Soviet and Russian security services (Cheka, OGPU, NKVD, KGB, FSB) to influence the course of world events, in addition to collecting intelligence and producing "politically correct" assessment of it. Active measures range "from media manipulations to special actions involving various degrees of violence". They include disinformation, propaganda, counterfeiting official documents, assassinations, and political repression, such as penetration into churches, and persecution of political dissidents. Active measures also include the establishment and support of international front organizations (e.g. the World Peace Council); foreign communist, socialist and opposition parties; wars of national liberation in the Third World; and underground, revolutionary, insurgency, criminal, and terrorist groups. The intelligence agencies of Eastern Bloc states also contributed to the program, providing operatives and intelligence for assassinations and other types of covert operations.

Ambiguity - the quality of being open to more than one interpretation; inexactness.

Analogous – (Analogy) a similarity between like features of two things, on which a comparison may be based.

Artificial Intelligence - the capacity of a computer to perform operations analogous to learning and decision making in humans

Attack vectors - a path or means by which a hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

Bitcoin – a type of digital currency in which a record of transactions is maintained and new units of currency are generated by the computational solution of mathematical problems and operates independently of a central bank.

BlackEnergy - a Trojan that is used to conduct DDoS attacks, cyber espionage and information destruction attacks.

Blackhat hackers - refers to a hacker who breaks into a computer system or network with malicious intent. A blackhat hacker may exploit security vulnerabilities for monetary gain; to steal or destroy private data; or to alter, disrupt or shut down websites and networks.

Black market - an illegal traffic or trade in officially controlled or scarce commodities.

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

Blockchain - a digital, public ledger that records online transactions. Blockchain is the core technology for cryptocurrencies like bitcoin. A blockchain ensures the integrity of a cryptocurrency by encrypting, validating, and permanently recording transactions. A blockchain is similar to a bank's ledger, but open and accessible to everyone who utilizes the cryptocurrency it supports.

Botnet - a group of computers connected in a coordinated fashion for malicious purposes. Each computer in a botnet is called a bot. These bots form a network of compromised computers, which is controlled by a third party and used to transmit malware or spam, or to launch attacks.

Cipher - a secret or disguised way of writing; a code.

Cloud storage - a service model in which data is maintained, managed, backed up remotely and made available to users over a network (typically the Internet).

ColdFusion - a product from the developer Macromedia, is a popular and sophisticated set of products for building Web sites and serving pages to users.

Computer Network Attack (CNA) - an offensive operation executed through the use of computer networks. The objective is to disrupt, deny, degrade, or destroy the information stored on computers and networks, or the actual computers and networks themselves.

Computer Network Exploitation (CNE) - CNE is primarily used within military institutes and organizations. It is a type of cybersecurity operation and can be considered equivalent to the jobs/processes of real-world spies or agents. It consists of techniques and processes that utilize computers or computer networks to penetrate targeted systems and networks.

Computer worm - a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth,

Cryptocurrency – a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

Cryptoworm – a form of malware that spreads in the form of a worm and encrypts victims' data.

Cyber-attack - an attempt to damage, disrupt, or gain unauthorized access to a computer, computer system, or electronic communications network.

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

Cyber-espionage - cyber spying, or cyber espionage, is the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of proxy servers, cracking techniques and malicious software including Trojan horses and spyware.

Cyber Operations (CO) - the employment of cyberspace capabilities when the primary purpose is to achieve objectives in or through cyberspace.

Cyber-persona layer - comprised of the personnel operating the terminals or workstations connected to the network. A cyber-persona is the digital representation of a user on the network.

Cyber proxy – an intermediary that conducts or directly contributes to an offensive cyber operation that is enabled knowingly, actively or passively, by a beneficiary who gains advantage from its effect. Also known as cyber mercenary.

Cyberspace - the global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cyber Security - precautions taken to guard against crime that involves the Internet, especially unauthorized access to computer systems and data connected to the Internet.

Cyber warfare - the use of computers and other devices to attack an enemy's information systems as opposed to an enemy's armies or factories. Essentially, warfare between states, albeit conducted in the cyber realm. It consists of states (and state-sponsored agencies) launching cyber-attacks against each other.

Cyber warrior - a computer expert engaged in the infiltration or sabotage of information systems, or in the defense of information systems against outside attack, typically for strategic or military purposes.

Database - a structured set of data held in a computer, especially one that is accessible in various ways.

Distributed Denial of Service (DDoS) - an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.

De-escalation - reduction of the intensity of a conflict or potentially violent situation.

Deface - spoil the surface or appearance of (something), for example by drawing or writing on it.

Defensive Cyber Operations (DCO) – the CO we execute to defend DoD cyberspace assets and capabilities. They include active and passive defense operations, and afford us the ability to utilize our capabilities in this domain.

Degrade - to reduce an adversary's cyberspace capability and the ability to accomplish their mission.

Deny - to prevent the adversary or target of an operation from being able to utilize their cyberspace capabilities.

Department of Defense information networks (DODIN) - a set of globally interconnected information capabilities used to collect, process, disseminate and manage classified and unclassified data, making it readily available to joint users.

Destroy - to cause irreparable damage to an adversary's asset.

Disrupt - to temporarily interfere with the normal operation of an adversary's cyberspace assets.

Encrypt - convert (information or data) into a cipher or code, especially to prevent unauthorized access.

Espionage - the use of spies by a government to discover the military and political secrets of other nations.

Flame malware - also known as Flamer, sKyWIper, and Skywiper, is modular computer malware discovered in 2012 that attacks computers running the Microsoft Windows operating system. The program is being used for targeted cyber espionage in Middle Eastern countries.

Firewall - a part of a computer system or network which is designed to block unauthorized access while permitting outward communication.

Forensics - scientific tests or techniques used in connection with the detection of crime.

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

Geostrategic - a subfield of geopolitics, is a type of foreign policy guided principally by geographical factors as they inform, constrain, or affect political and military planning.

Guardians of Peace – a hacker organization that claims to have participants worldwide. It is suspected to have first attacked SONY Corporation on November 24, 2014 and subsequently hacked SONY on December 5, 2014

Hacker - a person who uses computers to gain unauthorized access to data.

Hacktivists - a person who gains unauthorized access to computer files or networks in order to further social or political ends.

Homogeneous - composed of parts or elements that are all of the same kind; not heterogeneous: A homogeneous population.

Hybrid warfare – a military strategy which employs political warfare and blends conventional warfare, irregular warfare and cyberwarfare with other influencing methods, such as fake news, diplomacy, lawfare and foreign electoral intervention.

Informationized warfare - a concept involving the battlespace use and management of information and communication technology (ICT) in pursuit of a competitive advantage over an opponent. Information warfare is the manipulation of information trusted by a target without the target's awareness so that the target will make decisions against their interest but in the interest of the one conducting information warfare. As a result, it is not clear when information warfare begins, ends, and how strong or destructive it is. Information warfare may involve the collection of tactical information, assurance(s) that one's own information is valid, spreading of propaganda or disinformation to demoralize or manipulate the enemy and the public, undermining the quality of the opposing force's information and denial of information collection opportunities to opposing forces.

Insider trading - the illegal practice of trading on the stock exchange to one's own advantage through having access to confidential information.

Internet Protocol (IP) - the principal set (or communications protocol) of digital message formats and rules for exchanging messages between computers across a single network or a series of interconnected networks

Korea Herald - a daily English-language newspaper founded in 1953 and published in Seoul, South Korea

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

Lawfare - a form of war consisting of the use of the legal system against an enemy, such as by damaging or delegitimizing them, tying up their time or winning a public relations victory.

Local File Inclusion (LFI) breach – a hacking technique used to trick the web application into exposing or running files on the web server.

Logical network layer - encompasses the digital relationships or associations that exist on a network. The Air Force Portal is a perfect example.

Malformed Packets - packet mangling is the modification of packets at a packet-based network interface before and/or after routing.

Malicious - characterized by malice; intending or intended to do harm.

Cookies - a way for the website to recognize you and keep track of your preferences.

Malware - software intended to damage a computer, mobile device, computer system, or computer network, or to take partial control over its operation.

Man in the middle cyber-attack - a type of cyber-attack where a hacker intercepts the data passing between you and a website, app, or server.

Manipulate - to control or change the adversary's data, their information systems, and/or networks, in a manner that best supports our objectives.

Modus Operandi (M.O.) - a particular way or method of doing something, especially one that is characteristic or well-established.

Motherboard - a printed circuit board containing the principal components of a computer or other device, with connectors into which other circuit boards can be slotted.

Nation-state – sometimes referred to as "state", a sovereign state inhabited by a relatively homogeneous group of people who share a feeling of common nationality.

Network - a group of two or more devices that can communicate. In practice, a network is comprised of a number of different computer systems connected by physical and/or wireless connections.

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

Network-centric warfare - also called network-centric operations or net-centric warfare, is a military doctrine or theory of war pioneered by the United States Department of Defense in the 1990s. It seeks to translate an information advantage, enabled in part by information technology, into a competitive advantage through the robust computer networking of well-informed geographically dispersed forces.

Non-State actors (NSAs) - individuals or groups that hold influence and which are wholly or partly independent of a sovereign state or state.

NotPetya - a malware infection that targeted Windows computers in Ukraine. Introduced in 2017, and alleged to be from Russia, NotPetya malware spread across Europe causing billions of dollars' worth of damage.

Offensive Cyber Operations (OCO) – the CO intended to project power by the application of force in and through cyberspace.

Open-source software (OSS) - a type of computer software in which source code is released under a license in which the copyright holder grants users the rights to study, change, and distribute the software to anyone and for any purpose.

Packets - the unit of data that is routed between an origin and a destination on the Internet or any other packet-based network.

Packet-based network – a network that uses packets, or groups of packets, to transfer and receive digital information.

People's Liberation Army (PLA) - The armed forces of the People's Republic of China (PRC) and its founding and ruling political party, the Communist Party of China (CPC).

Phishing cyber-attack - to try to obtain financial or other confidential information from Internet users, typically by sending an email that looks as if it is from a legitimate organization, usually a financial institution, but contains a link to a fake website that replicates the real one.

Physical network layer – comprised of a geographic component and physical network component. The physical network component consists of the actual hardware, software and infrastructure that make up the network.

Plausible deniability - the ability of people (typically senior officials in a formal or informal chain of command) to deny knowledge of or responsibility for any damnable actions committed

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

by others in an organizational hierarchy because of a lack of evidence that can confirm their participation, even if they were personally involved in or at least willfully ignorant of the actions.

Provocative - doubtfulness or uncertainty of meaning or intention.

Pseudonyms - a fictitious name, especially one used by an author.

Qriocity - (pronounced as curiosity) is a trading name for Sony Corporation's streaming music, games, e-books and video on demand services.

Random Access Memory (RAM) - a type of data storage used in computers that is generally located on the motherboard. This type of memory is volatile and all information that was stored in RAM is lost when the computer is turned off.

Ransomware – a type of malicious software designed to block access to a computer system until a sum of money is paid.

Script kiddies - in programming and hacking culture, a script kiddie, skiddie, or skid is an unskilled individual who uses scripts, or programs developed by others, to attack computer systems and networks and deface websites.

Supervisory Control and Data Acquisition (SCADA) - SCADA generally refers to an industrial computer system that monitors and controls a process. In the case of the transmission and distribution elements of electrical utilities, SCADA will monitor substations, transformers and other electrical assets. SCADA systems are typically used to control geographically dispersed assets that are often scattered over thousands of square miles.

Social engineering - a form of techniques employed by cybercriminals designed to lure unsuspecting users into sending them their confidential data, infecting their computers with malware or opening links to infected sites.

Solvency - the ability of a company to meet its long-term debts and financial obligations. Solvency is essential to staying in business as it demonstrates a company's ability to continue operations into the foreseeable future.

Source Acknowledgment – the placement of a superscript number immediately following a title, statement or phrase (i.e.…"title[7]").

Source code - a text listing of commands to be compiled or assembled into an executable computer program.

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

Sovereignty - the full right and power of a governing body over itself, without any interference from outside sources or bodies.

Spam - irrelevant or inappropriate messages sent on the Internet to a large number of recipients.

Structured Query Language (SQL) injection - a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution

State actors - In United States law, a state actor is a person who is acting on behalf of a governmental body, and is therefore subject to regulation under the United States Bill of Rights, including the First, Fifth and Fourteenth Amendments, which prohibit the federal and state governments from violating certain rights and freedoms.

Statecraft - the art of government and diplomacy.

Stuxnet - Stuxnet is a malicious computer worm, first uncovered in 2010, thought to have been in development since at least 2005. Stuxnet targets SCADA systems and is believed to be responsible for causing substantial damage to Iran's nuclear program.

Tactics, Techniques and Procedures (TTPs) - in the context of cyber threat intelligence is also sometimes referred to as Tools, Techniques, and Procedures. TTPs are representations of the behavior or modus operandi of cyber adversaries. It is a term taken from the traditional military sphere and is used to characterize what an adversary does and how they do it in increasing levels of detail.

The Onion Router (Tor) - an open-source software program that allows users to protect their privacy and security against a common form of Internet surveillance known as traffic analysis.

Trojan horse virus - a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems.

Unabridged - has not been reduced in size by omission of terms or definitions; the most comprehensive version.

Unrestricted Warfare - transcends all boundaries and limits of traditional warfare. For the Chinese, these include psychological warfare, media warfare and legal warfare.

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

Via - traveling through (a place) en route to a destination.

Volatile - used to describe memory content that is lost when the power is interrupted or switched off.

WannaCry – a ransomware cryptoworm that targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham

Reference Materials

1. "Joint Publication 3-12(R), Cyberspace Operations." 5 February 2013. https://fas.org/irp/doddir/dod/jp3_12r.pdf
2. "Joint Publication 6-0, Joint Communications System." 10 June 2015. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6_0.pdf
3. Poirer, William J, and James Lotspeich. "Air Force Cyber Warfare." Air & Space Power Journal, 2013, pp. 73–97., www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-27_Issue-5/F-Poirier_Lotspeich.pdf.
4. "Russia Military Power." Defense Intelligence Agency, 2017, www.dia.mil/Military-Power-Publications/.
5. Connel, Michael, and Sarah Vogler. Russia's Approach to Cyber Warfare - Cna.org. CNA Analysis & Solutions, Mar. 2017, www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.
6. Kehler, C. Robert, et al. "Rules of Engagement for Cyberspace Operations: a View from the USA." Journal of Cybersecurity, 28 Mar. 2017, doi:10.1093/cybsec/tyx003. https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyx003/3058505
7. Van Ruitenbeek, Elizabeth, et al. Characterizing the Behavior of Cyber Adversaries: The Means, Motive, and Opportunity of Cyberattacks. University of Illinois, www.perform.illinois.edu/Papers/USAN_papers/10VAN01.pdf.
8. Williams, Brad D. "Profiles in Cyber: Understanding the US's Major Adversaries in Cyberspace." Fifth Domain, Fifth Domain, 26 May 2017, www.fifthdomain.com/home/2017/05/26/profiles-in-cyber-understanding-the-uss-major-adversaries-in-cybersapce/.
9. Vavra, Shannon. "The World's Top Cyber Powers." Axios, 13 Aug. 2017, www.axios.com/the-worlds-top-cyber-powers-1513304669-4fa53675-b7e6-4276-a2bf-4a84b4986fe9.html.
10. "TOP 10 of the World's Largest Cyberattacks." Outpost 24 Blog, 3 Dec. 2018, outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks. https://outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks.

COORDINATION	
AUTHOR	Mr. Burleigh, 23 Jan 2018 // Reviewed/Updated 23 July 2019 by Mr. Kirkham