Course Code	COMP 20333
Course Title	Social and Professional Issues in IT
Week Number	08
Reporters (Group No. 6)	Blances, Edsel Ian Tampi Camba, Michael Cariño Mangilinan, Aizen Louise Valentino
Topic	Information Warfare • Cyber Espionage • Intelligence Gathering
Learning Outcomes	Understand professional, ethical, legal, security and social issues and responsibilities in the utilization of information technology

Information Warfare

Information warfare (IW) represents a rapidly evolving and, yet imprecisely defined field of growing interest for defense planners and policymakers. The source of both the interest and the imprecision in this field is the so-called information revolution—led by the ongoing rapid evolution of cyberspace, microcomputers, and associated information technologies. The U.S. defense establishment, like U.S. society, is moving rapidly to take advantage of the new opportunities presented by these changes. At the same time, current and potential U.S. adversaries (and allies) are also looking to exploit the evolving global information infrastructure and associated technologies for military purposes.

Information Warfare in its broadest sense is a struggle over the information and communications process, a struggle that began with the advent of human communication and conflict. Over the past few decades, the rapid rise in information and communication technologies and their increasing prevalence in our society has revolutionized the communications process and with it the significance and implications of information warfare. Information warfare is the application of destructive force on a large scale against information assets and systems, against the computers and networks that support the four critical infrastructures (the power grid, communications, financial, and transportation). However, protecting against computer intrusion even on a smaller scale is in the national security interests of the country and is important in the current discussion about information warfare.

Experts tend to associate information warfare with U.S. military and espionage systems, while other national systems may use different terminology. In terms of practical implementation, information warfare was practiced in earlier times. For example, during the industrial age, airplanes would cover villages or towns with leaflets or materials as part of foreign policy implementation. As the industrial age progressed to the age of radio and television, this type of media was used in information warfare.

Today, nearly all relevant implementations involve digital media. Examples of modern information warfare include offensive strategies to invade or hobble an enemy’s IT infrastructure, as well as efforts to defend IT systems against cyberattacks.

Types of information warfare include:

- Using viruses or malware for cyberattacks
- Exploiting holes in a network
- Stealing information through various types of unauthorized access

The Origins of Information Warfare

Some historians hold that information warfare dates from the beginning of the 20th century, noting, for example, that the French army conducted IO activities in the First World War, using electronic warfare techniques that enabled the interception of wireless and telephone communications. Yet, history confirms otherwise - appreciation for the value of intelligence dates to Sun Tzu and earlier, and 18th and 19th century leaders conducted information warfare using information-related intelligence gathering, military deception, military information support operations, and operations security. Examining these roots of modern-day information operations can yield valuable insights.

Why is Information Warfare created?

The chief objective of information warfare is to achieve information superiority over an adversary. It might mean more information; it does mean better information. IW means making sure our information is reliable and accurate. At the same time, IW means denying information superiority to an adversary. This could mean denying information or manipulating the information available to an adversary. The playing field is "info-space" the collection of all things involved in generation, gathering, processing, storage, and transmission of information. IW holds that the information a nation's military has

available to decide will, to a large extent, determine its activities. If that information can be controlled, so can the resulting military actions.

Politics, Security, and IT

Talampas (2002), revealed in his study that the Politics, Security, and IT of the Philippines has a vibrant civil society and uncivil elements have both utilized the available technology to test the limits of expression and liability in the country. They have both demonized public and private figures and Institutions. Such a situation like the "love bug" controversy failed to confine the issue to the legal arena but may have also emboldened the nefarious activities. Philippine internal security forces have had their taste of cyber vandalism as the police website was hacked but other examples of electronic fraud have remained confidential. Computer-based disaster and emergency response and sea transport surveillance systems have been unevenly utilized in keeping civilian deaths tolls down. Their security counterparts have been annoyingly embroiled in the embattled political landscape.

Cyber Espionage

Espionage, according to Merriam-Webster, is "the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company."

Take this into the cyber world, and the spies are armies of nefarious hackers from around the globe who use cyber warfare for economic, political, or military gain. These deliberately recruited and highly valued cybercriminals have the technical know-how to shut down anything from government infrastructures to financial systems or utility resources. They have influenced the outcome of political elections, created havoc at international events, and helped companies succeed or fail.

Cyber espionage, or cyber spying, is a type of cyberattack in which an unauthorized user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons.

Cyber spying is a cybercrime and is sometimes referred to as cyber espionage. It is when hackers target computers or IT networks to gain access to information that may be personal or classified. This information is typically in digital format and is somehow profitable for hackers.

Cyber spying is an advanced concept. As technology has advanced so has the history of cyber spying events. The definition provided above can get a little confusing without understanding the basics. Understanding cyber spying is easier with the definitions of another computer lingo. Webopedia refers to cybercrime as "any criminal act dealing with computers and networks". This can include any crime such as slander, harassment, or hate crimes. However, it is most associated with stealing information from computers. The term hacker is often misconstrued. Webopedia defines hacker as "a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject". The word hacker is carrying a negative weight because the media interpreting it wrong. Over time, the new definition of the word that has been created is "individuals who gain unauthorized access to computer systems for the purpose of stealing". This can also be referred to as cracker.

Cyber Espionage Targets

The most common targets of cyber espionage include large corporations, government agencies, academic institutions, think tanks or other organizations that possess valuable IP and technical data that can create a competitive advantage for another organization or government. Targeted campaigns can also be waged against individuals, such as prominent political leaders and government officials, business executives and even celebrities.

Cyber spies most commonly attempt to access the following assets:

- Research & Development data and activity
- Academic research data
- IP, such as product formulas or blueprints
- Salaries, bonus structures and other sensitive information regarding organizational finances and expenditures
- Client or customer lists and payment structures
- Business goals, strategic plans, and marketing tactics
- Political strategies, affiliations, and communications
- Military intelligence

Industry Pulse: Who's Gaining Fame as the Most Nefarious of All?

So, what have the Masters of Cyber Espionage been up to lately? Here are a few of the nation-state attack groups that have been headlined repeatedly over the years.

North Korea

North Korea reportedly has an army of more than 6,000 hackers that raise money to pay for the country's nuclear program. A recent attack attributed to North Korea is APT37, which took aim at South Korea, Japan, Vietnam, and the Middle East. The attack was purportedly led by a well-known hacking group called Lazarus, which has been active for the last five years or so. The group has been cited for attacks such as the Sony Pictures one in 2014, which netted tens of millions of dollars, and it may be responsible for the $81 million cyber heist of a Bangladeshi bank in 2016. They also are blamed for the 2017 widespread WannaCry attack, which wreaked billions of dollars of havoc on companies, banks, and hospitals around the world.

Vietnam

Onto Vietnam, and there is OceanLotus, a cyber espionage group which could potentially be behind the attacks called APT32 and APT-C-00. These threats have been aimed at corporate and government organizations in Vietnam, the Philippines, Laos, and Cambodia and focus on foreign corporations with interests in Vietnam's manufacturing, consumer products, and hospitality industries.

China

One of China's well-known attack groups is TEMP.Periscope, or Leviathan. This group has recently been escalating their attacks and targeting U.S. companies in the engineering and maritime fields that are linked to the South China Sea and some of the world's busiest trading routes. Another group of Chinese threat actors, APT10, is blamed for a campaign that perhaps started as early as 2009. As potentially one of the longest sustained cybersecurity threats in history, APT10 recently attacked companies through managed service providers in multiple industries in several countries, as well as some Japanese companies, causing an unknown amount of damage through the theft of large volumes of data.

Another potential nation-state attack is Slingshot APT, which may have links back to the government of the United States. Slingshot APT has similarities to a threat actor known as Grey Lambert or Longhorn, which has been linked to the U.S.'s CIA. The campaign may have been active for six years or more and targeted the Middle East and Africa via sophisticated evasive and stealthy tactics that help the actors successfully exfiltrated large volumes of sensitive data.

Lazarus may be responsible for a $81M cyber heist on a Bangladeshi bank that occurred in 2016.

The purpose of Cyber Espionage

Cyber espionage is primarily used to gather sensitive or classified data, trade secrets or other forms of IP that can be used by the aggressor to create a competitive advantage or sold for financial gain. In some cases, the breach is simply intended to cause reputational harm to the victim by exposing private information or questionable business practices.

Cyber espionage attacks can be motivated by monetary gain; they may also be deployed in conjunction with military operations or as an act of cyber terrorism or cyber warfare. The impact of cyber espionage, particularly when it is part of a broader military or political campaign, can lead to disruption of public services and infrastructure, as well as loss of life.

Common Cyber Espionage Tactics

Most cyber espionage activity is categorized as an advanced persistent threat (APT). An APT is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network to steal sensitive data over a prolonged period. An APT attack is carefully planned and designed to infiltrate a specific organization and evade existing security measures for long periods of time.

Executing an APT attack requires a higher degree of customization and sophistication than a traditional attack. Adversaries are typically well-funded, experienced teams of cybercriminals that target high-value organizations. They've spent significant time and resources researching and identifying vulnerabilities within the organization.

Most cyber espionage attacks also involve some form of social engineering to spur activity or gather needed information from the target in order to advance the attack. These methods often exploit human emotions such as excitement, curiosity, empathy, or fear to act quickly or rashly. In doing so, cybercriminals trick their victims into giving up personal information, clicking malicious links, downloading malware or paying a ransom.

Other common attack techniques include:

- **Watering hole**: Malicious actors are able to infect legitimate websites commonly visited by the victim or people associated with the target with malware for the explicit purpose of compromising the user.
- **Spear-phishing**: A hacker targets specific individuals with fraudulent emails, texts, and phone calls in order to steal login credentials or other sensitive information.

- **Zero-day exploits**: Cybercriminals leverage an unknown security vulnerability or software flaw prior to discovery and patching by the software developer or the customer's IT team.
- **Inside actors or insider threat**: A threat actor convinces an employee or a contractor to share or sell information or access to the system to unauthorized users.

Global Impact of Cyber Espionage

Cyber espionage, particularly when organized and carried out by nation states, is a growing security threat. Despite a rash of indictments and legislation intended to curb such activity, most criminals remain at large due to a lack of extradition agreements between countries and difficulty enforcing international law related to this issue. This issue, combined with the growing sophistication of cyber criminals and hackers, leaves open the possibility for a coordinated and advanced attack that could disrupt any number of modern-day services, from the operation of the electricity grid to financial markets to major elections.

Cyber Espionage Penalties

While many countries have issued indictments related to cyber espionage activity, the most serious cases usually involve foreign actors in countries that are not subject to extradition. As such, law enforcement agencies are relatively powerless to pursue cybercriminals, particularly those operating abroad. That said, the investigative groundwork used to support cyber espionage indictments can also be used as the basis for sanctions imposed on a foreign country or company. For example, in the U.S., the Department of the Treasury may use investigative material from indictments to level economic sanctions against a corporation that has known involvement in cyber espionage activity.

Cyber Espionage Detection, Prevention and Remediation

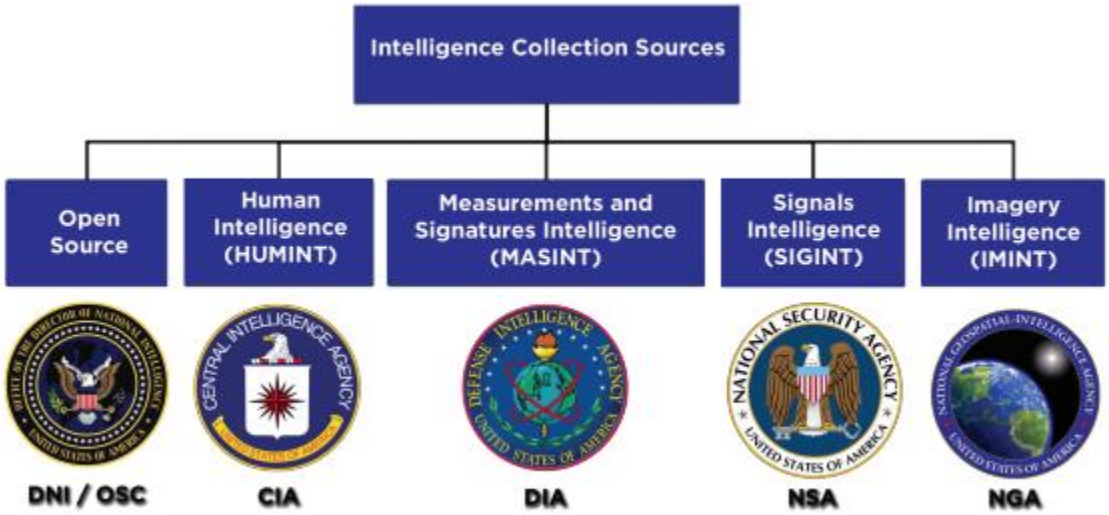
The growing sophistication of cyber attackers and cyber spies has enabled them to bypass many standard cybersecurity products and legacy systems. Although these threat adversaries are often highly advanced and can leverage complex tooling in their operations, defending against these attacks is not a lost cause. There are many cybersecurity and intelligence solutions available to assist organizations in better understanding the threat adversaries, their attack techniques, and the tradecraft they regularly employ.

- **Sensor Coverage**. You can't stop what you don't see. Organizations should deploy capabilities that provide their defenders with full visibility across their environment, to avoid blind spots that can become a safe haven for adversaries.
- **Technical Intelligence**. Leverage technical intelligence, such as indicators of compromise (IOCs), and consume them into a security information and event manager (SIEM) for data enrichment purposes. This allows for added intelligence when conducting event correlation, potentially highlighting events on the network that may have otherwise gone undetected. Implementing high-fidelity IOCs across multiple security technologies increases much-needed situational awareness.
- **Threat Intelligence**. Consuming narrative threat intelligence reports is a sure-fire method for painting a very vivid picture of threat actor behavior, the tools they leverage and the tradecraft they employ. Threat intelligence assists with threat actor profiling, campaign tracking and malware family tracking. These days, it is more important to understand the context of an attack rather than just knowing an attack itself happened, and this is where threat intelligence plays a vital role.
- **Threat Hunting**. Understanding technology will only get organizations so far is more important now than ever before. Many organizations will find the need for 24/7, managed, human-based threat hunting to accompany their cybersecurity technology already in place
- **Service Provider**. Partnering with a best-of-breed cybersecurity firm is a necessity. Should the unthinkable happen, organizations may require assistance responding to a sophisticated cyber threat.

Intelligence Gathering

Intelligence gathering can be dissected into different modes of which Open Source Intelligence, Cyber Intelligence, and Human Intelligence are the most viable for targeted attacks. Open-source Intelligence is the process of gathering intelligence from publicly available resources (including Internet and others). OSINT should not be confused with Open Source Software (OSS) as these are both different elements. The presence of "Open Source" is used distinctively in OSINT and OSS but refers to the same standards which are publicly available resources and software. CYBINT is the process of explicitly gaining intelligence from available resources on the Internet. CYBINT can be considered as a subset of OSINT. HUMINT is the process of gaining intelligence from humans or individuals by analyzing behavioral responses through direct interaction. OSINT, CYBINT, and HUMINT are used for both legitimate and nefarious purposes. In this report, we concentrate on intelligence gathering modes within cyber space. However, HUMINT definition can be extended with respect to Internet in which intelligence is gathered through e-communication by interacting with individuals through video sharing, messaging, etc.

Five Main Ways of Intelligence Gathering



- **Human Intelligence (HUMINT)** is the collection of information from human sources. The collection may be done openly, as when FBI agents interview witnesses or suspects, or it may be done through clandestine or covert means (espionage). Within the United States, human intelligence collection is the FBI's responsibility. Beyond U.S. borders, human intelligence is generally collected by the CIA, but also by other U.S. components abroad. Although human intelligence is an important collection discipline for the FBI, they also collect intelligence through other methods, including signals intelligence, measurement and signatures intelligence, and open-source intelligence.

- **Signals Intelligence (SIGINT)** refers to electronic transmissions that can be collected by ships, planes, ground sites, or satellites. Communications Intelligence is a type of signals intelligence and refers to the interception of communications between two parties. U.S. signals intelligence satellites are designed and built by the National Reconnaissance Office, although conducting U.S. signals intelligence activities is primarily the responsibility of the National Security Agency (NSA).

- **Imagery Intelligence (IMINT)** is sometimes also referred to as photo intelligence. One of the earliest forms of imagery intelligence took place during the Civil War, when soldiers were sent up in balloons to gather intelligence about their surroundings. Imagery Intelligence was practiced to a greater extent in World Wars I and II when both sides took photographs from airplanes. Today, the National Reconnaissance Office designs, builds, and operates imagery satellites, while the National Geospatial-Intelligence Agency is largely responsible for processing and using the imagery. Geospatial Intelligence is the analysis and visual representation of security related activities on the earth. It is produced through an integration of imagery, imagery intelligence, and geospatial information.

- **Measurement and Signatures Intelligence (MASINT)** is a relatively little-known collection discipline that concerns weapons capabilities and industrial activities. Measurement and Signatures Intelligence includes the advanced processing and use of data gathered from overhead and airborne imagery intelligence and signals intelligence collection systems. Telemetry Intelligence is sometimes used to indicate data relayed by weapons during tests, while electronic intelligence can indicate electronic emissions picked up from modern weapons and tracking systems. Both telemetry and electronic intelligence can be types of signal intelligence and contribute to measurement and signatures intelligence.

- **Open-Source Intelligence (OSINT)** refers to a broad array of information and sources that are generally available, including information obtained from the media (newspapers, radio, television, etc.), professional and academic records (papers, conferences, professional associations, etc.), and public data (government reports, demographics, hearings, speeches, etc.).

Intelligence Gathering Methods

- Intelligence gathering methods
- Interception of telecommunications
- Intelligence gathering in lieu of interception of telecommunications
- Telecommunications surveillance
- Procurement of base station data

- Technical hardware monitoring
- Transmission reproduction
- Network traffic intelligence
- Systematic monitoring
- Covert intelligence gathering
- Acquiring intelligence that identifies a telecommunications address or terminal hardware
- Undercover operations
- Undercover purchasing
- Guided human intelligence operations
- Duplication
- Intercepting a dispatch for the purpose of duplication
- On-site audio monitoring
- On-site visual monitoring
- Technical surveillance
- Intelligence gathering on specific locations

Ethical Issues of Intelligence Gathering

The root of the ethical problem over the collection of intelligence lies in the need to overcome the determined will of the person with the secret not to allow it to be known. Inevitably this leads to individuals being treated and where necessary manipulated as means to the end of acquiring the information. That is true whether they are being recruited as agents having their privacy rights interfered with by any number of different kinds of technical operations including bugging of dwellings and vehicles or monitoring of personal communications or simply deceived by the everyday tradecraft of the spy.

The purpose of Intelligence Gathering

Intelligence gathering plays a major role in today's warfare as intelligence provides us with knowledge about what the enemy may be doing or is going to do in the future. Intelligence can be about enemy weapons, troop strengths, troop movement activity, and future operational plans, to name just a few. Intelligence gathering techniques are widely varied from human informants on the ground to satellites orbiting the earth and taking photographs of targeted locations.

REFERENCES

_____. (n.d.). Intelligence gathering. Supo. https://supo.fi/en/intelligence-gathering

_____. (n.d.). LibGuides: Intelligence Studies: Home. https://usnwc.libguides.com/c.php?g=494120

_____. (n.d.). What is Cyber Espionage?. vmware. https://www.vmware.com/topics/glossary/content/cyber-espionage.html

Baker, K. (2022). What is Cyber Espionage?. ***CrowdStrike***. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

Bastian, N.D. (2019). Information Warfare and Its 18th and 19th Century Roots. The Cyber Defense Review. https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2017786/information-warfare-and-its-18th-and-19th-century-roots/

CrowdStrike. (2022). What is Cyber Espionage?. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

Grimmick, R. (2022). What is Cyber Espionage? Complete Guide with Protection Tips. https://www.varonis.com/blog/what-is-cyber-espionage

Jones, A., et.al. (2013). Cyber Spying. https://www.cs.odu.edu/%7Etkennedy/cs300/development/Public/M11-17970Week11-Ethics/index.html

Molander, R.C., et.al. (1996). Strategic Information Warfare: A New Face of War. RAND Corporation. https://doi.org/10.7249/MR661

Omand, D. (2021). The Ethical Limits We Should Place on Intelligence Gathering as Part of an Integrated CT Strategy. *Terrorism and Political Violence*, *33*(2), 290–301. https://doi.org/10.1080/09546553.2021.1880225

Sood, A., & Enbody, R. (2014). Targeted Cyber Attacks: Multi-Staged Attacks Driven by Exploits and Malware. Elsevier Gezondheidszorg.

Talampas, R. (2002). Is there Information Warfare in Southeast Asia? *Kasarinlan: Philippine Journal of Third World Studies*, *17*(2), 51–68. https://www.journals.upd.edu.ph/index.php/kasarinlan/article/view/690

Techopedia. (2017). Information Warfare. ***Techopedia.com***. https://www.techopedia.com/definition/29777/information-warfare