The Role of Digital Forensics in Spectrum Warfare

Dauda Sule, CISA

Air Force Institute of Technology, Kaduna, Nigeria

Abstract

Rapid developments in information and communications technology have resulted in increased innovations in terms of warfare. From World War II signal technology like jamming became mainstay in warfare; electronic warfare became virtually an integral part of war. By the 2000's there was an increasing use of cyberspace in warfare (i.e. cyber warfare) and the emergence of attacks like Stuxnet which did not target information systems, but physical infrastructure; and tensions between Russia and its neighbors resulting in Ukraine's power grid being brought down by Russian cyber-attacks. As at 2019 the US Army merged its electronic warfare and cyber warfare operations as a result of developments in the battle spectra.

Digital forensics has a key role to play in modern day warfare. Digital forensics tools can be used for monitoring and intelligence, as well as investigating how an attack was carried out. Digital forensics can greatly improve a nation's dominance of the electromagnetic spectrum giving it the upper hand whether in terms of defense or offense.

Background

The extensive use of electronic jamming methods from the dawn of World War II led to some of the early battles involving Britain and the Nazis being referred to by Winston Churchill as Battle of the Beams (Rambo, 2009). World War II heralded the extensive use of electronic methods in modern warfare, such that even in times of peace, the techniques are continually upgraded and personnel constantly trained to ensure preparedness in the event war breaks out.

Spectrum warfare or electronic warfare (EW) was defined by Adamy (2004) as the art and science of preserving the use of the electromagnetic spectrum for friendly use while denying its use to an adversary; essentially spectrum warfare involves manipulation of the electromagnetic spectrum in such a way as the ensure a nation or entity has an upper hand over adversaries. Developments in information technology, especially the Internet, birthed another advancement in warfare: cyberwarfare. Cyberwarfare is a significant aspect of electronic warfare which some may erroneously be inclined to think is the only part of electronic warfare that is important in modern times. However, whether or not cyberwarfare is involved, virtually all aspects of battle equipment are one way or the other linked to information systems and devices. These systems and devices generate footprints in the form of electronically stored information (ESI) which can be used to trace how an event may have taken place, by who, from where and when. In recent times, inculcation of cyberwarfare into electronic warfare has led to electronic warfare being referred to as “spectrum warfare” (both terms may be used interchangeably in this presentation).

Digital forensics tools are used to analyze electronic footprints (ESI) in order to unravel events and incidents, but also they can be applied for intelligence gathering. Data can be gathered

from both friendly and adversary sources to unravel incidents and also for reconnaissance. For example, a network that was compromised could be investigated using digital forensics to discover the source of such an attack and how it was successful, the data can be used to strengthen the network against future attacks as well. Another example is the recovery of an adversary's drone which could be used to gain insight into the adversary's capabilities and can also be re-engineered to monitor and gather intelligence on them.

Introduction to Spectrum Warfare

Spectrum warfare which may also be referred to as electronic warfare (EW) can simply be defined as the manipulation of the electromagnetic spectrum (EMS) in a way that favors a nation state against its adversaries, giving the nation an upper hand in warfare. Von Spreckelsen (2018) gave NATO's definition of EW as military action that actively and passively exploits electromagnetic energy to provide situational awareness and create offensive and defensive effects. The electromagnetic spectrum is vital for modern communication, especially in battle situations. The manipulation of this spectrum is the main point of EW, manipulation to protect infrastructure or to be used against an adversary in an offensive manner.

The electromagnetic spectrum involves all types of light – whether visible to the human eye (rainbow colors) or not. The electromagnetic spectrum was defined by Schneider (1993) as a continuum of all electromagnetic waves arranged by wavelength and frequency, and electromagnetic energy is radiated from celestial bodies at various wavelengths at the speed of light ($3x10^5$ kilometers per second). The wavelength of the waves is inversely proportional to the frequency and energy. There are seven regions in the EMS, namely: radio waves, microwaves, infrared (IR), visible light, ultraviolet (UV), X-rays, and gamma rays.

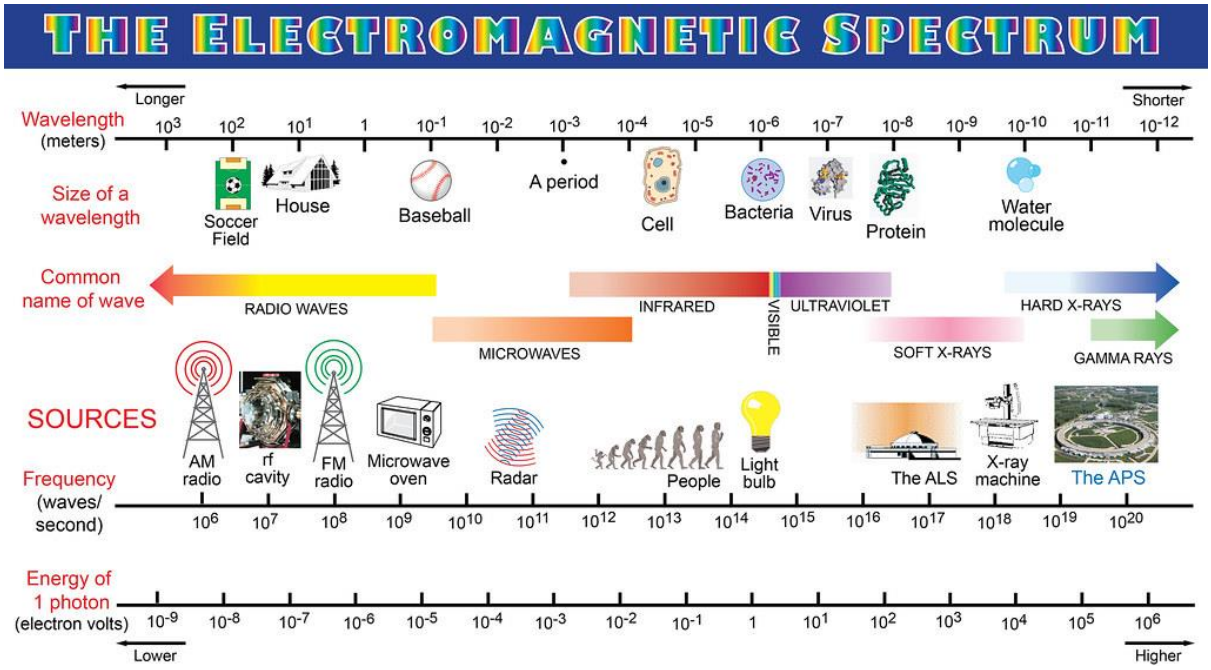

Figure 1: *"Electromagnetic Spectrum" by AdvancedPhotonSource is licensed under CC BY-NC-SA 2.0*

The electromagnetic spectrum is vital for modern communication, especially in battle situations. The manipulation of this spectrum is the main point of EW, manipulation to protect infrastructure or to be used against an adversary in an offensive manner. Reconnaissance missions can be carried out by nations states or any other adversary by passively monitoring electronic waves; for example, using network sniffers to observe network traffic, flying aerial vehicles (manned or unmanned) towards borders of hostile nations to get radar data, and so on. These can be used to understand the capabilities of the adversary; hence create awareness on being alert against them, and also provide intelligence on how to successfully attack or thwart their infrastructure.

The EMS can additionally be used to disseminate information in such a way that an adversary is misled or put in a state of confusion. This can be achieved by using decoys, sending false signals or even transmitting misleading information through airwaves like TV, radio and

through cyberspace over various social media platforms. Information warfare, psychological warfare and cyber warfare can be seen as subsets of EW, although some may categorize them as being independent of EW. Cyber warfare tends to be considered separate from EW as it applies to network based communication, taking advantage of system flaws and using manipulative techniques like social engineering to gain access to targeted systems; while EW has traditionally focused on managing the EMS to one's advantage for defense, offense, detection and degradation of an adversary's EMS use (Stephens, 2014). However, Stephens (2014) argued that all area networks utilizing wireless communication (whether WiFi or Bluetooth) utilize the EMS; and that furthermore networks connected via coaxial or fiber optic cables transfer data by way of electrical circuits which are waves of voltage and current - they are electromagnetic waves. This led him (2014) to conclude that the difference between cyber and electronic warfare was just the medium of transferring signals. The fact that the US Army merged its electronic warfare functional area into its Cyber Branch (Cox et al 2019) further buttresses this point.

Historical Milestones in the Development of Spectrum Warfare

US Civil War

In 1844 Samuel Morse sent the first telegraph, two decades later it was adopted as a means of communication that covered long distances quicker than the then norm by the US military - this provided an advantage to the Union armies, but was subject to wiretapping by the confederates (LaMarche, n.d.). This could be seen as one of the earliest iterations of EMS being adopted in warfare; the Unionist used it to give them an upper hand over the confederates, who in turn could intercept it and use the information obtained for countermeasures.

Russo-Japanese War

Next was during the Russo-Japanese war in 1905, where a Japanese warship had detected the Russian fleet and was communicating its location to the Japanese fleet headquarters in Korea using radio frequency; the communication was intercepted by the Russians. The Captain of the Russian ship that intercepted the communication wanted to jam the signal to distort the message to their enemy's headquarters, but the Admiral of the fleet rejected the offer (Rambo, 2009). At the end of the day the Japanese defeated the Russians.

World War I

When World War I broke out, there was already need for quick communication over long distances, hence improvements in the development of signals intelligence. The British had severed undersea cables used for communication by the Germans forcing them to adopt telegraph and radio communications, and also increased their use encryption for the purpose as these means of communication were susceptible to interception (LaMarche, n.d.).

In 1917, the visible light spectrum was adopted for EW by way of the dazzle camouflage. The dazzle camouflage was created by a Royal Navy volunteer reserve called Lieutenant Norman Wilkinson (Kiger, 2019) which turned the concept of camouflage on its head. During that period German U-Boats were most feared in the sea, they were submarines that could easily sneak up on ships and take them out with torpedoes, the need to camouflage British ships became imminent so Wilkinson brought the idea of a camouflage that would not hide ships, but rather make them even more conspicuous. The concept was to paint the ships in zebra stripes which used the visible light spectrum to confuse the Germans. The zebra stripes made it difficult to determine the size, speed and distance of the ships which were required for

targeting; not being able to determine the correct location and speed of the ships made it difficult for torpedoes to target them.

World War II

In a buildup to World War II British forces had developed warning signals to detect German fighter planes if they crossed their airspace by use of radio transmitters - radar (Verdict Media Limited, 2018). The Germans also developed transmitter systems to guide landing and bombing at night from which the British developed countermeasures for – jamming. The transmitters used beams to steer bombs to their targets, once over the target they would receive a tone, the British employed higher frequency transmitters that superimposed on the German's frequency rendering them unusable (LaMarche, n.d.). The British also employed similar transmitters for bombing the Germans, but these were also susceptible to jamming; additionally, the Germans used radar to detect British planes. The British resorted to a countermeasure of amplifying radar signals and retransmitting to the Germans, giving the illusion of one plane being more than one, such that it could serve as a decoy. The Germans went on to use additional radar frequencies to counter the allies' countermeasures which led the allies resorting to jamming communications between radar operators and the German fighter planes instead (LaMarche, n.d.). The wide use of radio frequencies and radar by both the allied and axis forces during the early battles led to Winston Churchill referring to them as "the battle of the beams" (Rambo, 2009).

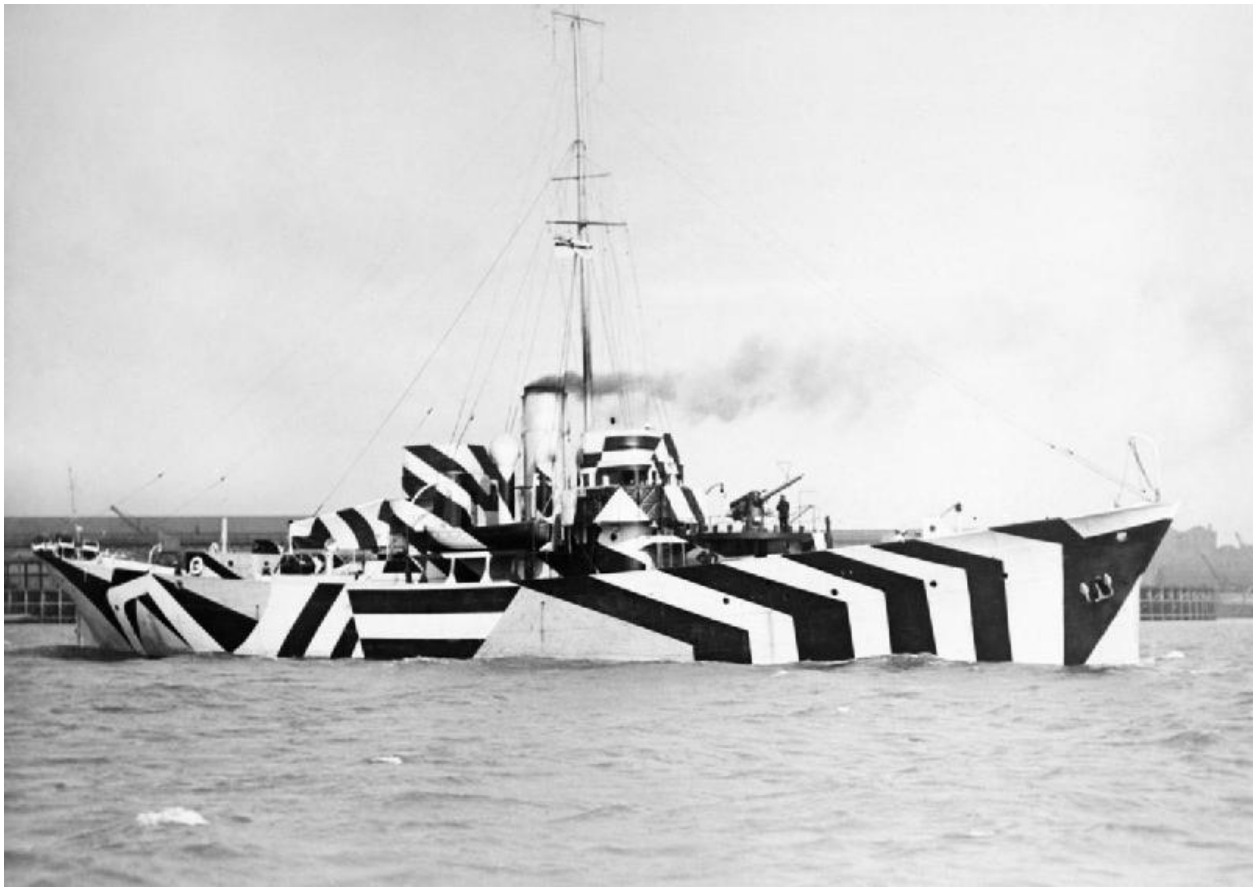

Figure 3: Picture from 1918 of HMS Kildangan gunboat painted in dazzle camouflage

Arab-Israeli Wars

The Israelis defeated the Egyptian Air Force during the Six Day War in 1967 by means of EW. This was achieved by jamming the most distant Egyptian radar within range of the Israeli forces in addition to infiltrating Egyptian Air Defense radio communications, sending misleading instructions and canceling correct ones causing pandemonium for the Egyptians (Rambo, 2009).

The Israelis also adopted EW against the Syrians in the Battle of Latakia during the Yom Kippur War, 1973. It was an encounter between missile-boats (the first such encounter in history, and also the first use of EW for such) where the Israelis used electronic countermeasures to

jam the Syrian missile guidance systems resulting in the destruction of the Syrian ships (Verdict Media Limited, 2018).

US Military from Late '80s to the Second Gulf War

The US Air Force has used stealth aircraft as countermeasures against enemy radar. Two F-117 Nighthawk stealth aircraft were used to bomb Rio Harto airfield during the 1989 invasion of Panama, the planes were also deployed during the 1991 Gulf War (Verdict Media Limited, 2018). Global position system (GPS) was also deployed during the Gulf War for tracking targets and missile guidance, but was susceptible to countermeasures by unsophisticated jamming methods used by the Iraqis (Verdict Media Limited, 2018). The US Army used Long Range Acoustic Devices (LRAD) in the second Gulf War to disperse crowds at checkpoints; crowds were potential targets for suicide attacks (Niiler, 2018).

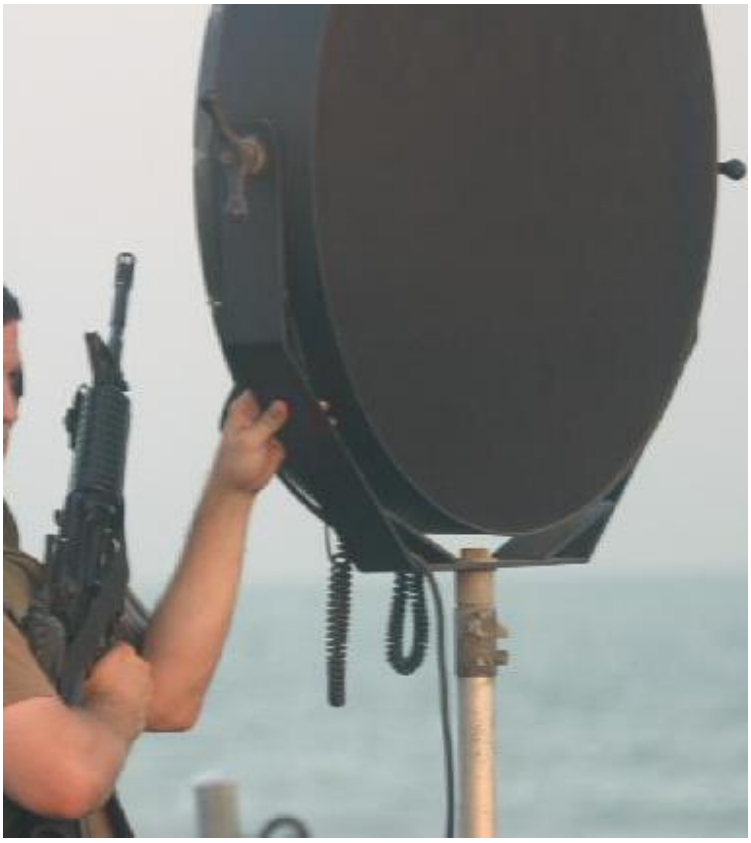

Figure 4: US Navy LRAD

Stuxnet

Stuxnet, the malware was detected in 2010, but thought to have been installed in 2005; it could be seen as the first case of cyber warfare deployment. It is suspected that the malware which adversely affected the Iranian uranium enrichment program was a collaborative operation by the US and Israel. The Iranian nuclear processing plants had gone off the Internet to avoid such an attack, but the malware was able to spread on their local area network by means of infected USB storage devices. This was also a milestone in terms of a cyber-attack having a direct effect on physical infrastructure.

Suspected Russian Attacks 2014 - 2019

In 2014 and 2016, Ukraine's power grid was brought down by cyber-attacks purportedly from Russia (Brumfield, 2019). There were also allegations that Russia meddled in the US 2016 presidential elections by using social media disinformation to influence voters' way of view; resulting in the election of President Trump - this encompassing cyber, information and psychological warfare aspects of EW.

According to Stubbs and Bing (2019) Russian cyber-attack unit was also accused of carrying out cyber-attacks against others by hacking an Iranian spying operation making it look like the Iranians were behind the attacks. This kind of operation can result in countries or entities fighting each other not knowing that their conflict was initiated by a different country or entity.

Israeli Response to Hamas Hacking Unit 2019

The response of the Israeli Defense force's strike against Hamas' hacking unit in real-time, 2019, was another major milestone in cyber warfare and the tendency for cyber and physical warfare to converge (Newman, 2019) - a real-time physical response. The challenge of this

kind of physical response is that it can be manipulated by a third party, like the Russian hacking of an Iranian operation making it appear Iran was behind attacks could have resulted in a physical strike against Iran.

US Patrol Aircraft hit over Philippine Sea 2020

In the first quarter of 2020 the US accused China of using a laser not visible to the human eye to target a US naval patrol aircraft over the Philippine Sea (Mabeus, 2020). China denied carrying out an attack against the American aircraft. This revolves around the use of lasers for EW which can be used to jam aircraft signals causing damage to the plane, leading to it crashing, being captured or rendering its attack and defense capabilities useless.

Figure 5: US Navy Laser Weapon System

Future Trends in Spectrum Warfare

Verdict Media Limited (2018) made mention of developments in force-fields and cloaking devices, like what obtains in Hollywood movies, that as of 2014 Karlsruhe Institute of Technology had developed light-bending matter that could become invisible in foggy weather; and that Boeing had as at 2015 filed a patent for an electromagnetic arc that could serve as a force-field to protect vehicles and buildings from being damaged by a blast - the force-field is created by superheating air with an arc generator that creates a plasma shield that is denser than air.

There has also been development of so called “suicide drones” by some countries (like Israel and Turkey). The Israelis developed Harop as a Suppression of Enemy Air Defenses (SEAD) weapon (Rogoway, 2016) and the Turks have a squad of swarming drones known as Kargus (Trevithick, 2020). The kamikaze drones can work together and coordinate attacks, they can carry out attacks and return, or they can become missiles themselves to blow up targets.

L3Harris Technologies, Inc. (2020) observed that with improvements in technology and the ease of getting tools for EW in current times, it is incumbent that superiority be maintained to survive in modern warfare by constant and proactive improvement and innovation. Constant training, simulation and upgrading to meet up with modern realities and technology are compulsory to ensure survival in EW.

Functions of Spectrum Warfare

Components

Electronic warfare has three components:

- electronic attack (EA)

- electronic protection (EP)
- electronic support (ES).

Electronic Attack

Electronic Attack(EA) is the offensive use of the EMS against an adversary. L3Harris (2020) described EA as an integral part of a military operation employed to achieve superiority over an adversary by suppressing their air defenses and disrupting their communication; that is to deny the adversary ability to communicate, navigate, locate targets and/or gather intelligence. Victoria (2019) defined an electronic attack as activities that aim to prevent or minimize the adversary's use of the EMS, as well as destroy, neutralize or degrade their combat capability by targeting their own EW emissions using electromagnetic tools. So essentially EA is used to counter the enemy's EMS application for warfare in order to gain an upper hand against them.

EA can be non-destructive (soft kill) or destructive (hard kill); two classifications. The soft kill EA are carried out without resulting in physical damage to the adversary, usually causing interference to impede their operations or limiting the use of their electronic equipment or impeding their decision making process or sending misleading messages and instructions. Popularly used methods are jamming of signals and the like. Jamming was used a lot during World War II, in fact until recently soft kill was the only EA. Most of the methods used before the 2000's were soft kill EA.

Hard kill EA is destructive. It aims to cause physical damage to the adversary. Hard kill EA can also be subdivided into Direct Energy Emission and Target Emission Weapon Guidance. Direct Energy Emission involves use of direct electromagnetic emissions that are high powered to cause physical damage. Examples include electromagnetic pulse that can be

used to bring down an aircraft; and laser beams like the one the US accused China of using as in the first quarter of 2020 to target a US naval patrol aircraft over the Philippine Sea. Target Emission Weapon Guidance use self-sensing systems that take advantage of the adversary's electromagnetic emissions used for guiding their weaponry to target and destroy the systems (Victoria, 2019). Examples of Target Emission Weapon Guidance are anti-missile systems like those deployed against Intercontinental Ballistic Missiles (ICBM).

Electronic Protection

Electronic Protection (EP) as the name implies, is used for countering EA in order to protect infrastructure from an adversary's EW application. The United States Air Force (2002) defined EP as actions taken to protect personnel, facilities and equipment from any EW employment by an adversary meant to degrade, neutralize or destroy friendly combat capability. Victoria (2019) gave a definition of EP as the component of EW that encompasses actions taken to ensure effective use of the EMS, notwithstanding the actions of an adversary, friendly forces or unintended interference; that is to say EP is the effective management of the EMS to avoid it been exposed to manipulation by an adversary whether by direct action of the adversary or misapplication by own forces that the adversary can take advantage of.

EP seeks to deny the adversary the ability to monitor, intercept, track or analyze EMS transmissions from friendly forces; ensuring the adversary does not gain an upper hand. EP also helps reduce the impact of enemy EA to the barest minimum. EP can be achieved by managing electromagnetic emissions by use of tools and equipment that protect; and controlling the emissions to avoid detection and interference.

Electronic Support

United States Air Force (2002) defined Electronic Support (ES) as response to tasks for searching, intercepting, identifying and locating sources of intentional and unintentional radiated electromagnetic energy for the purpose of threat recognition. ES are used to gather and analyze necessary information from the EMS regarding activities of adversaries and even friendly forces to guide actions to be taken whether for attack or defense. Signals intelligence (SIGINT) can be used to enhance ES. ES ensures effective and efficient use of the EMS (Victoria, 2019). ES can be employed both during war and times of peace, it is of passive nature. Information from ES can be used for situational awareness; for training and simulation. Hence it can be used to improve upon EA and EP capabilities.

ES involves gathering information about an adversary's activities from their transmissions and emission in the EMS. The information gathered from searching, monitoring and locating the adversary's position and activities; then gathered information is then analyzed possibly in conjunction with other intelligence data gathered (like from signals intelligence - SIGINT) to get an idea of what the adversary is up to. The analysis could be of communication content (what is being communicated within the adversary's forces); the communication traffic could be analyzed to understand the pattern flow and direction locate and track transmission devices; technical analysis of the communication and comparison with what was previously collected to identify who might be using communicating with whom.

Data and information gathered and analyzed from the EMS about an adversary can be used to determine the location strength and capability of the adversary and also what they may be planning to in order to counter and overcome them.

Tenets

Spectrum Warfare has the following three tenets which guide its functionality:

- Control
- Exploit
- Enhance

Control

EW is defense and offense based, usually working in the form of move and countermove - that is to say actions are taken as an independent step or in response to another action taken by an adversary (United States Air Force, 2002). These actions of taking a measure or countering a measure usually occur at the same time, having domination of the EMS ensures control allowing freedom and ease of maneuver and out-maneuver of the adversary. EW is meant to ensure control of the EMS to ensure there is an upper hand against the adversary.

An example of taking control was shown in the defeat of Egypt's Air Force by the Israelis in the Six-Day War, where they were able to dominate the Egyptians EW and manipulate it against the Egyptians leading to their defeat.

Exploit

Of course the point of having control over the EMS is to be able to exploit to one's advantage against an adversary. EW exploits the EMS to detect, deny, disrupt, destroy in various ways to impede an adversary's decision taking and maneuver (United States Air Force, 2002); hence EW exploits the EMS to ensure defeat of an adversary by being ahead of

them in the form of detecting their movements and acting before they can make a move or reaction and also throwing them into a frenzy, leaving them in a state of pandemonium.

Signal jamming that was carried out by the British against the Germans was a use of EW to exploit the EMS in favor of the British in World War II. Still referring back to Israel versus Egypt in the Six-Day War, the Israelis effectively exploited the EMS against the Egyptian Air Force by intercepting their communications and sending them misleading instructions.

Enhance

The United States Air Force (2002) stated that to enhance is to make EW a force multiplier. That is to say proper application of EW by taking control of and exploiting the EMS in one's favor, the effectiveness and success of military operations will be greatly enhanced.

The dazzle camouflage used in World War II enhanced the operations of British ships against German U-Boats, helping them get past the Germans and have more successful movement. The Israelis also enhanced their successes in their battles against the Egyptians in the Six-Day War and the Syrians in the Yom Kippur War.

Conclusion

The main functions of EW is to use the EMS against an adversary in attack, countering their own use; defending against attacks by an adversary, countering their countermeasures; and for support in terms of communication, guidance, intelligence and reconnaissance.

To summarize, EW helps to ensure control of the EMS in order to exploit it to enhance success in military operations. These objectives can be achieved by means of intelligence, which will enhance support (ES) that can be used to attack (electronic attack - EA) or defend against attacks (electronic protection - EP).

Digital Forensics in Military Terms

ES can be seen as the bedrock for successful electronic warfare. ES involves gathering and analysis of data for preparation against attacks or to carry out offensive action; digital forensics can be used to enhance ES by gathering and analyzing ESI from digital devices which includes from computer systems, networks, unmanned vehicles, mobile devices and so on. ES gathers information using the same methods and techniques as signals intelligence (SIGINT) and communications security (COMSEC). SIGINT is intelligence gathered from the adversary's emissions in the electromagnetic spectrum, while COMSEC is from friendly forces (own forces and allies). ES uses COMSEC to enhance security of friendly forces electromagnetic emissions by unravelling vulnerabilities and loopholes then strengthening to prevent exploitation by adversaries. SIGINT has three fields:

- Communications intelligence (COMINT): this involves interception of enemy's human-intelligible communications like phone calls, text messages, audio and visual messages, and so on, for intelligence analysis.

- Electronic intelligence (ELINT): this involves gathering data regarding electronic emissions that are not human-intelligible from the electromagnetic spectrum for intelligence analysis. These are emissions from things like radar and other weapons systems in order to get an understanding of enemy capabilities.

- Foreign Instrumentation Signals Intelligence (FISINT): The Central Intelligence Agency (2010) described FISINT as signals detected from weapons under testing and development. It is used to gain intelligence on what weapons an adversary is developing.

There is an obvious need for information collection and gathering in spectrum warfare, whether for ES, COMSEC or SIGINT. This seeks to show how digital forensics can be used to enhance spectrum warfare capabilities with increased and improved data collection and analysis in the light of increased used of computerized systems and networks in warfare and civil operations. The civil operations are also at risk of attack, can be from hostile nation states or terrorists, anarchists and so on.

It is clear that spectrum warfare helps to ensure control of the electromagnetic spectrum in order to exploit it so as to enhance having an upper hand over adversaries. These objectives can be achieved by means of intelligence, which will enhance support measures (ES) that can be used to attack (EA) or defend against attacks (EP).

ES overlaps SIGINT which also gathers and analyses adversarial emissions for intelligence analysis. According to Haig (2015), ES can be used to provide SIGINT as they both use the same resources and data collection methods; only that the intent for collecting and usage as well as level of analysis may not be the same. So essentially ES is the main data collection aspect of spectrum warfare, whether for SIGINT or COMSEC, which will be used to further protect infrastructure or to get an upper hand over an adversary. This where digital forensics comes in.

Digital forensics can be seen as the practice of collecting, analyzing and reporting on digital data (Kavrestad, 2018) that can be used to prove or gain better understanding of an event or device/equipment (like mobile phones, network logs, unmanned aerial vehicles, and so on). Easttom (2019) gave a definition from the Computer Emergency Response Team as the process of using scientific knowledge for collecting, analyzing and presenting evidence to courts, dealing primarily with recovery and analysis of latent data. The latter definition

mentions courts of law, however, in military iterations, this may not necessarily be the case. Guarino (2013) also offered a definition by Pearson (2001) that digital forensics is the use of scientifically derived and proven methods to preserve, collect, validate, identify, analyze, interpret, document and present digital evidence in order to reconstruct events found to be criminal or helping to anticipate unauthorized actions that are proven to be disruptive to planned operations. This definition given by Guarino (2013) is more encompassing and involves its use for preventative/defensive measures as opposed to the more widely accepted definitions of digital forensics which emphasize legal acceptability of the methods of collecting the evidence and the evidence itself as apparent form the Computer Emergency Team's definition. Guarino (2013) pointed out that digital forensics in a warfare situation varies from civilian usage in that the main point of use in civilian terms is forensic soundness of the evidence (the evidence has to be legally acceptable from collection to presentation), while in military terms there is more emphasis and need for actionable intelligence requiring tight turn-around-time. However, Giordano and Macaig (2002) observed that there is still a need for the digital evidence to be legally acceptable as it might be required if against a civilian perpetrator as there might be need to legally justify any action against such an actor(s) in the light of international laws, treaties or agreements. This point was also buttressed by Guarino (2013) mentioning that contemporary international relations require nation-states providing justifiable evidence for carrying out actions against other nations, organizations or individuals (like providing evidence to the United Nations or the International Criminal Court of Justice).

Giordano and Macaig (2002) defined digital forensics in a military context as the exploration and application of scientifically proven methods to collect, process, interpret and utilize digital evidence for the purpose of providing conclusive description of cyber-attack activities

against one's infrastructure for recovery and restoration of critical aspects; correlating, interpreting and predicting actions of adversaries and how they impact planned military operations; and ensuring data is forensically sound to be presented in court for legal cases. From the foregoing definition it can be seen that digital forensics can be used for disaster recovery and continuity, intelligence and legal evidence in the military context; gathering of digital evidence for these purposes amounts to security intelligence.

Security intelligence according to Rouse (2015) is the information required to protect an organization from internal and external threats and in addition the processes, policies, and tools designed to gather and analyze the information. The Recorded Future Team (2020a) also defined security intelligence as an outcomes-centric approach to minimizing risks that fuses internal and external threat, security, and business insights across an entire organization by unifying collection, analysis and as well as data automation and insights. ELINT is one of the ways this kind of intelligence can be gathered from electronic emissions alongside COMINT for human communications. Use of digital data gathered using digital forensics in military applications amounts to security intelligence it has a broad range of applications to ultimately protect and secure a nation and its infrastructure. May (2020) mentioned two types of security intelligence:

- Operational/technical security intelligence: this provides knowledge on ongoing attacks, events and campaigns leading to specialized insights as to the nature, intent, and timing of specific attacks as they take place. It is usually sourced from devices and equipment and includes technical data and information about attacks like the methods applied and vulnerabilities exploited.; hence also known as technical security intelligence. This can be easily applied using artificial intelligence.

- Strategic security intelligence: this provides a wide scale overview of an organization's (or nation state's, in this case) threat landscape and is used for taking high-level decisions and is usually presented through briefings and reports. It requires high-level management experience and expertise to successfully analyze and interpreted the threat landscape, hence artificial intelligence would generally not be applicable for analysis. However, some automation would still be required to sort large volumes intelligence source material before the human analysis and interpretation.

The intelligence source material need to be collected and analyzed using tools that combine them into a single source, deduplicate and remove false positives, make necessary comparisons and generate automatic alerts (May, 2020). According to May (2020), security intelligence has a six phase life cycle:

- Direction: here goals are set for the security intelligence program based on a proper understanding of the capabilities and threat landscape.
- Collection: gathering of relevant digital evidence from various sources.
- Processing: converting the collected evidence into formats that are easily and readily accessible and assessable.
- Analysis: interpreting the processed evidence into actionable intelligence, exposing what was deduced.
- Dissemination: sending the intelligence output to the appropriate authorities for decision making.

- Feedback: input by the decision makers made on how to further improve on intelligence supplied and adjustments that may arise due to changing needs.

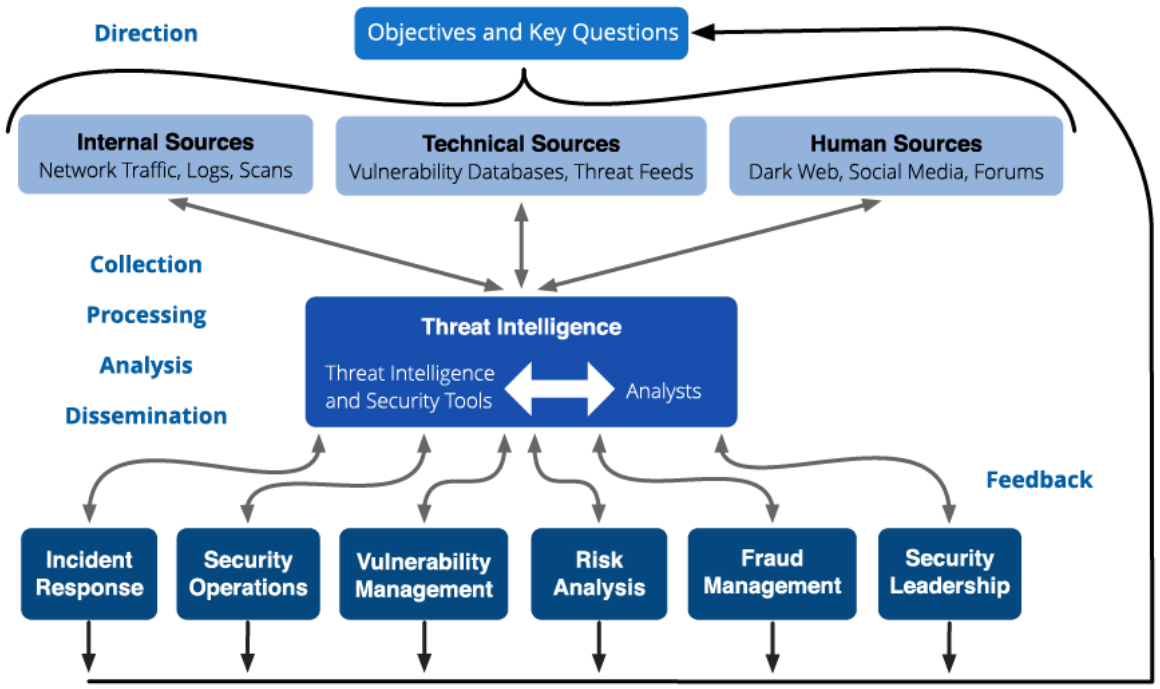

Figure 6: Threat Intelligence and the 6 Phases of the Security Intelligence Cycle (Source: *The Recorded Future Team, 2020*)

These phases are similar to phases of the digital forensics process and understanding that helps improve the process. The digital forensics process has the following phases:

- Identification: knowing what will be relevant digital evidence and where to source it from.
- Collection: gathering the relevant evidence from identified sources.
- Preservation: ensuring the collected evidence is not tampered with, damaged or destroyed. Can involve converting to easily accessible format.

- Analysis: interpreting the preserved evidence.
- Presentation: forwarding the deduced findings to the relevant authorities for appropriate action.

Suffice to say digital forensics can be used to meet up security intelligence which can be used to enhance spectrum warfare, specifically through ES and SIGINT. The digital intel can be used to better defend friendly electromagnetic and non-electromagnetic communications (COMSEC), protect friendly forces based of situation analysis of adversary capabilities, countering adversary's attack and defense measures by disrupting, and degrading their discovered capabilities; these are some of the functions of electronic warfare mentioned by Haig (2015).

References

Adamy, D.L (2004). EW 102: A Second Course in Electronic Warfare. *Artech House, Boston.*

Brumfield, C. (2019, November, 22). Russia's Sandworm Hacking Group Heralds New Era of Cyber Warfare. *CSO.* Retrieved from https://www.csoonline.com/article/3455172/russias-sandworm-hacking-group-heralds-new-era-of-cyber-warfare.html

Cox, J. et al (2019, Fall). The Friction Points, Operational Goals, and Research Opportunities of Electronic Warfare and Cyber Convergence. *Cyber Defense Review*. Retrieved from /Portals/6/Documents/CDR%20Journal%20Articles/Fall%202019/CDR%20V4N2-Fall%202019_COX-BENNET.pdf?ver=2019-11-15-104109-047#:~:text=ELECTRONIC%20WARFARE%20AND%20CYBER%20CONVERGENCE,-I.&text=On%20October%201%2C%202018%2C%20the,land%20operations%20and%20joint%20operations.

Easttom, C. (2019). Systems Forensics, Investigations and Response. *Information Systems Security & Assurance Series, Jones & Bartlett Learning, Burlington (3rd ed.)*

Giordano, J. and Macaig, C. (2002). Cyber Forensics: A Military Operations Perspective. *International Journal of Digital Evidence Summer 2002;1(2).* Retrieved January 07, 2021, from https://www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632B-FF420389C0633B1B.pdf

Guarino, A. (2013). Digital Forensics in a Cyber Warfare Context. *StudioAG – ICT Consulting & Engineering.* Retrieved January 07, 2021, from http://www.studioag.pro/wp-content/uploads/2013/03/DigitalForensicsAndCyberwarfare.pdf

Haig, Z. (2015). Electronic Warfare in Cyberspace. *Security and Defence Quarterly 2015;7(2):22-35*. https://doi.org/10.5604/23008741.1189275

Kavrestad, J. (2018). Fundamentals of Digital Forensics Theory, Methods and Real Life Applications. *Springer International Publishing AG.* https://doi.org/10.5604/23008741.1189275

Kiger, P.J. (2019, March 14). The WWII 'Dazzle' Camouflage Strategy Was So Ridiculous It Was Genius. *History.* Retrieved from https://www.history.com/news/dazzle-camouflage-world-war-1

LaMarche, M. (n.d.). The History of Electronic Warfare - Part 1. *Microwaves101.* Retrieved April 13, 2020, from https://www.microwaves101.com/encyclopedias/the-history-of-electronic-warfare-part-i

L3Harris Technologies, Inc. (2020). Electronic Attack. *L3Harris.* Retrieved May 15, 2020, from https://www.harris.com/content/electronic-attack

Mabeus, C. (2020, February 27). Pacific Fleet: Chinese Destroyer's Laser Targeted US Plane. *Navy Times.* Retrieved from https://www.navytimes.com/news/your-navy/2020/02/28/pacific-fleet-chinese-destroyers-laser-targeted-us-plane/

May, J. (Ed.) (2020). The Security Intelligence Handbook. *CyberEdge Press, Annapolis (3rd ed.).*

Niiler, E. (2018, August 27). Sonic Weapons' Long Noisy History. *History.* Retrieved from https://www.history.com/news/sonic-weapons-warfare-acoustic

Newman, L.H. (2019, May, 06). What Israel's Strike on Hamas Hackers Means for Cyberwar. *Wired.* Retrieved from https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

Rambo (2009, December 7). History of Electronic Warfare. Information Warfare. Retrieved from http://ew30.blogspot.com/2009/12/such-is-reliance-on-electromagnetic-em.html

Rouse, M. (2015). Security Intelligence (SI). *TechTarget.* Retrieved January 07, 2021, from https://whatis.techtarget.com/definition/security-intelligence-SI

Schneider, D.J. (1993). Electromagnetic Spectrum. Michigan Technical University. Retrieved March 26, 2020, from http://www.geo.mtu.edu/rs

Stubbs, J. and Bing, C. (2019, October 21). Hacking the Hackers: Russian Group Hijacked Iranian Spying Operation, Officials say. *Reuters.* Retrieved from https://www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1X00AK

The Recorded Future Team (2020a). Security Intelligence Definition: What it means for your Organization. *Recorded Future.* Retrieved January 07, 2021, from https://www.recordedfuture.com/security-intelligence-definition/

The Recorded Future Team (2020b, January 15). What the 6 Phases of the Threat Intelligence Lifecycle Mean for Your Team. *Recorded Future.* Retrieved from: What the 6 Phases of the Threat Intelligence Lifecycle Mean for Your Team (recordedfuture.com)

United States Air Force (2002, November 5). Electronic Warfare - Air Force Doctrine Document 2-5.1.

Verdict Media Limited (2018, June 7). The Evolution of Electronic Warfare: a Timeline. *Army Technology.* Retrieved from https://www.army-technology.com/features/evolution-electronic-warfare-timeline/

Victoria, A. (2019, October). Electronic Warfare. *Researchgate.* Retrieved from https://www.researchgate.net/publication/336473867_Electronic_Warfare

Von Spreckelsen, M. (2018). Electronic Warfare - The Forgotten Discipline. The Journal of Joint Air Power Competence Centre, 27. Retrieved March 26, 2020, from https://www.japcc.org/electronic-warfare-the-forgotten-discipline/