CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

DEVELOPMENT OF AN INTEGRATED OFFENSIVE CYBER COUNTER INTELLIGENCE CAPABILITY AS A CONCEPT

Col Rajnish Kumar Maahi, SM is an serving officer an alumnus of the Indian military Academy who was commissioned in Regiment of Artillery in 1999. The Officer in his illustrious career spanning over 23 years had a judicious mix of Command, Staff and Instructional appointments in varied operational environment. The officer is prep or PhD in Def & Strategic affairs with keen interest in cyber and Strategic Intelligence.

"Two things about the NSA stunned me right off the bat: how technologically sophisticated it was compared with the CIA, and how much less vigilant it was about security in its every iteration, from the compartmentalization of information to data encryption."

Edward Snowden

Abstract

The vulnerability highlighted by Edward Snowden in one of the most powerful intelligence gathering organisation with respect to guarding its own vulnerabilities which is a prevalent phenomenon in most of the organisations worldwide, including consequently in the Information age all the witness large strategies for cyber defence have evolved reactively after the lessons learnt post a large number of cyber attacks, spread over various geographic and time zones and diverse organisation worldwide. In addition, the uniquely selected cyber tools which are now being employed by the various state and non state actors for cyber attacks, render the prophylactic counter measures to be employed for securing the systems against these targeted

attacks, either are too expensive to operationalise, due to the high R&D and deployment costs or are rendered archaic, due to the dynamic and evolutionary technology and the pathways available to the persistent antagonists they have access to advanced system exploitation techniques and knowledge of existing but yet undiscovered software vulnerabilities. Which can be undertaken with small diversified and relatively averagely educated individuals across the globe. Therefore, in order to address these omnipresent threats caused by such antagonists, there is an urgent requirement for establishing a fast and offensive Cyber Counterintelligence (CCI) process, and a more efficient inter-organizational information exchange, under an equally effective and legally mandated organisation at national level. This paper proposes a conceptual framework for formulation of an offensive CCI, based on technical tools and techniques for data mining, anomaly detection, and extensive sharing of cyber threat data, under the legal ambit of a nation or organisation. The framework is placed within the distinct context of military intelligence, in a tri services domain order to achieve a holistic, offensive and target-centric view of future CCI. The main postulates of such a concept should include a comprehensive process that bridges the gap between the various actors involved in CCI, an applied technical architecture to support detection and identification of data leaks emanating from cyber espionage and deduced intelligence community requirements within the legal parameters of the organisation or a nation.

INTRODUCTION

The increasingly pervasive cyber environment of the information age allows seamless flow of information between organizations, systems and people diversified by time and space. The integration of physical processes, computation and information exchange has given rise to cyber-physical systems, supporting and facilitating human processes and needs in diverse areas as transportation, healthcare, financial, disaster response, government departments, non government organisations, research and entertainment to name a few. This phenomenon has been compounded and increased exponentially due the present COVID pandemic crisis, which has spread all across the globe. It can also be easily predicted that even, subsequent to the return to normalcy, this interconnecting of systems through common networks in the cyber domain, which has now become an indelible part of the routine efficiency and functionality, will be the new

normal. However, at the same time, it also raises new concerns in terms of data theft, frauds, cyber manipulation, misinformation, information operations and offensive cyber operations to name a few. Hence, this growing menace of malicious and transnational activities in cyberspace with low attributability and legality makes it challenging and difficult to address for both nations and organisations alike. In today's world, much of the open source information available with respect to organisations and institutions etc could be easily weaponised and used for strategic purposes by the adversary. These actions are a nightmare for the intelligence agencies as some of these assets might be under the private sector and even outside the realm of legal domain defined for that state or organisation.

Espionage committed by advanced actors with large resources, leveraging modern information and communications technology, is growing in frequency and scale. These actors are commonly labelled as Advanced Persistent Threats (APT). The recently published (2021) edition of the Verizon Data Breach Investigations Report [1] reveals that, while organized criminal groups are still the top actor category when it comes to causing data breaches, state-affiliated groups have now taken the number two spot. Actors within the latter category are not motivated by short-term financial gain, but are rather in pursuit of data that furthers specific national interests, such as military or classified documents, results from research and innovation, insider information or trade secrets, and technical resources such as source code. The "Mandiant Report"[2] published in April 2021 is another example of a recent, highly detailed study of the prevalence of this form of cyber espionage. It asserts that, over the last few years, over 140 organizations across the globe have been victims of advanced hostile cyber operations committed by a single antagonistic organization based in mainland China, involving systematic transfers of hundreds of terabytes of sensitive data across a diverse set of industries.[2, p. 20] While China is often accused of being the most active source of cyber espionage in the world today, recent (June 2013) disclosures[3] made by whistleblower Edward Snowden, a former member of the U.S. intelligence community, suggest that the U.S. government has also been conducting extensive so-called Offensive Cyber Effects Operations (OCEO) in order to further national objectives around the world.[4] The lack of adequate security measures against these types of highly sophisticated cyber operations is being reported as an increasingly urgent problem in many parts of the world. Whereas military organizations, government agencies and high-security

corporations traditionally have a high level of operational security awareness and thus may be somewhat better off, in regards to these threats, the most heavily affected organizations are those that are not accustomed to having information security considerations and risk management being an important part of their Routine business concerns.

Most of the organizations in group, in public as well as private sectors, continue to rely mainly on passive measures, such as firewalls and anti-virus software, to block out malicious traffic and software from their networks. In most cases regular system patching is seen as enough to correct vulnerabilities in installed software and to protect against zero-day exploits. While these approaches are effective against some threats, they fail to stop advanced attacks from an APT, and provide no knowledge of what such an adversary does once the network is penetrated. Moreover, much of the information security work being done within organisations and government sector is heavily compliance-driven, with a focus on living up to such information security management system standards as ISO/IEC 27000-series, as required by regulatory bodies.[5] The day-to-day efforts are centered on mitigating the continuous flow of discovered software vulnerabilities, patching servers, cleaning up infected clients, and getting back to business as usual. This has been perceived as the best approach to maintain business continuity, and to maintain the trust customers and the general public – where the main line of thought being that if you admit to being hacked, nobody would want to do business with you, or trust your ability to safeguard their sensitive data. Many cyber-incidents have thus been classified or otherwise concealed from public knowledge.

DEVELOPING A TARGET- CENTRIC CYBER COUNTERINTELLIGENCE MECHANISM

In the case of the relatively young field of CCI, two of the main challenges are that is hard to achieve is Situational Awareness (SA) and that the process of attaining positive attribution in limited time. Several of the experienced issues are a result of the overall game plan for CCI being inherited and adopted directly from conventional counterintelligence and traditional intelligence practices. The result is often seen in terms of extra focus on collection, while the and that “invisible walls” remain between collectors, analysts and consumers.[6] Another circumstance hampering the

CCI process is the traditionally strictly hierarchical intelligence cycle, requiring that higher echelons ask the “right” questions. However, this is something that is hard to fulfil within CCI since knowing what to look for demands specific knowledge and a very high level of domain expertise in several fields like technical, legal and cultural processes, demographic economic to name a few. The short time frames of cyberspace operations also put a higher demand on rapid reaction within the CCI process and on existing overburdened inter-organizational collaboration. A suggestive alternative model as given by Robert Clark[7]: in terms of development of target centric CCI existing model than the Evert centric model is shown in (see figure 1).

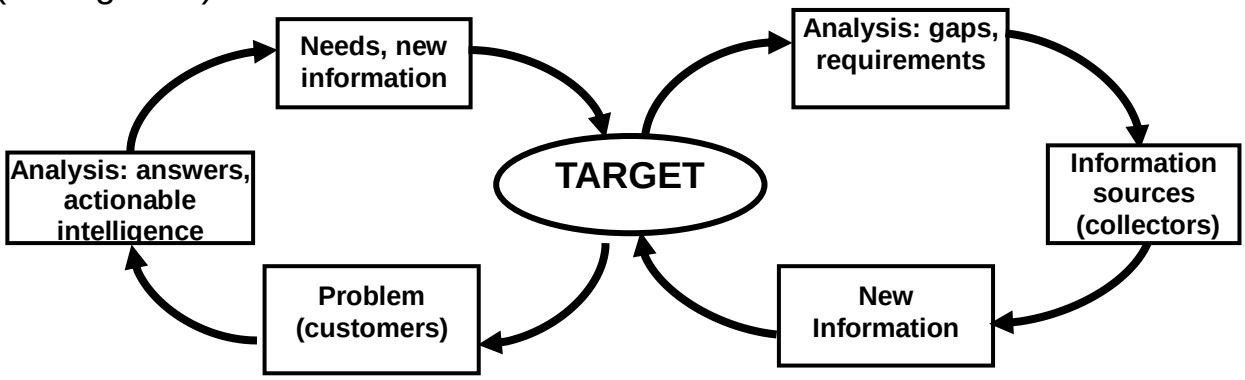

Figure 1. A target-centric view of the intelligence process

After adapting a target centric model of cyber intelligence the existing schema of CCI needs to be superimposed over the exiting multi domain target intelligence acquisition processes used by the various agencies.

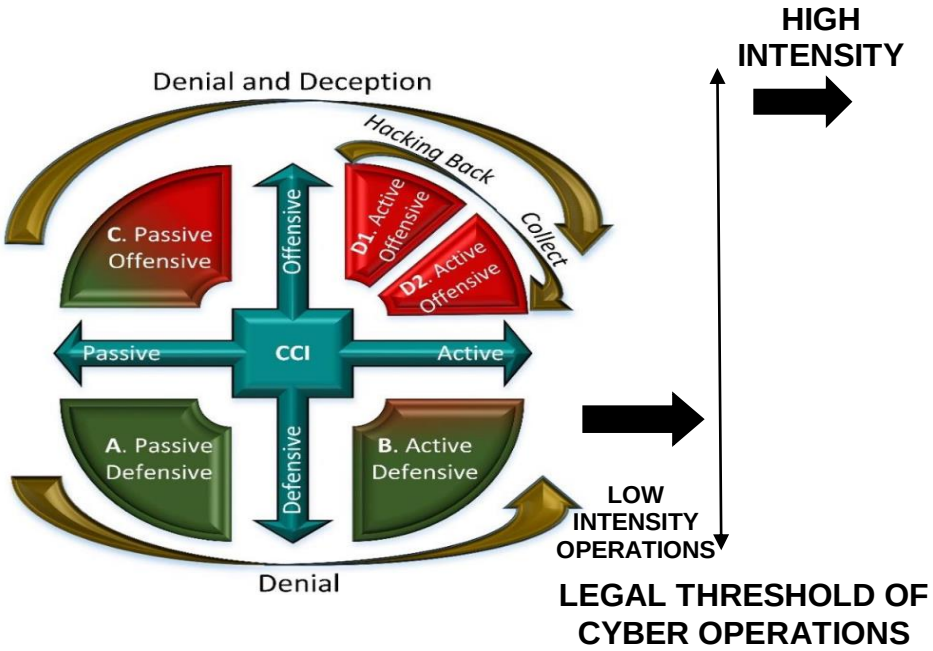

Figure 2: Various Quadrats Depicting the CCI Schema

Cyber Counter Intelligence (CCI) schema depicting The Quadrants of Cyber Counterintelligence – (Adapted from Sims 2009; Duvenage & von Solms 2015) as show in fig 2.

Within this adapted framework, it is possible to retain the initial four quadrants of counterintelligence. All four of these quadrants / dimensions (A, B, C and D) are then combined with the concept of denial and deception. Dimension A and B could focus on denial, and dimension C and D could focus on both denial and deception. The last dimension (D) then could also be further split in two, to allow for two unique focus areas within the active offensive dimension. This effectively splits the one dimension (dimension D) into two dimensions (Dimension D1 and D2), focussing either on hacking back (D1), or on cyber collection efforts (D2) - or on both of these areas (D1 and D2). This is done purposefully to allow for customisation later on within the maturity model based on an organisations area of business and profile (government, private sector etc.). In line with these modifications, the CCI framework then effectively consists of five dimensions. With the intention of being multi-disciplined, the CCIMM should also allow for the integration of existing cyber related defensive and/or offensive structures and efforts within an organisation. Each of the five dimensions are therefore broken down accordingly into three sub-dimensions, namely:-

- Strategic,
- Operational,
- Tactical

Each one of the sub-dimensions are then further broken down in six or more such areas of compliance (further described as categories), namely:-

- Structures,
- People,
- Processes,
- Technologies,
- Legal/ Policies,
- Training/ Skills Development.

These six categories could be identified as the main compliance focus areas, from the onset, that applicable to most of the prevalent environments irrespective, if it is a government department or private sector/Business etc. This does however not dictate that these are the only categories that can, or

should be utilised and additional sub categories like Bio surveillance, cognitive domain are etc could also be added.

Which categories can be identified and added based on the organisation's needs, nature of business and risk profile. Therefore, the level of adherence to each of the categories within a specific sub-dimension will be different to each organisation depending on the profile of the organisation (private sector business, government structure and so on). Accordingly, the intensity of adherence to the sub dimensions within each of the five specific dimensions will also differ from organisation to organisation, which would function under the legal framework and the mandated tasks assigned to them. Each of the six categories within the sub-dimensions are then allocated four levels of maturity, ranging from level 0 (indicating that nothing is in place) to Level 3 (the highest level of maturity). Every one of these maturity levels can be specified according to the need of the organisation, stemming from a defined baseline that is set for either a government environment or a private sector business environment. An organisation can then decide which level of maturity (level 0-3) it wishes to attain for each of the six categories within each sub-dimension for all five of the dimensions. This decision can be based on matters such as organisational strategy, risk profile and/or risk appetite, availability of funding, and so on. For all three sub-dimensions (under the five main dimensions), the six categories (as specified above) are the same, as each of these will need to comply with specific goals within each of the six categories. This also assists in aligning the corresponding categories within each of the three sub-dimensions throughout the five dimensions. The alignment is firstly done within each specific sub-dimension and then secondly between the five different dimensions to ensure that the five dimensions align with each other, as highlighted. It is based on the assumption that all stakeholders in the intelligence process (collectors, analysts, processers, technicians, and customers) need to participate actively. The goal is a more inclusive process where everyone contributes based on their individual knowledge and domain expertise in order to promote a more accurate picture of the target.[7] As the cyber espionage antagonist is commonly unknown, the target-centric view fits well with the task of focusing on attribution. An example of a system currently employing a target-centric view, in accordance with what Clark suggests, is Intellipedia – an online system for collaborative data sharing similar to that of the publicly available service Wikipedia, but limited to use by the U.S. intelligence community.[8]

The Flow Chart Could Further Illustrate the Same Concept As Under:-

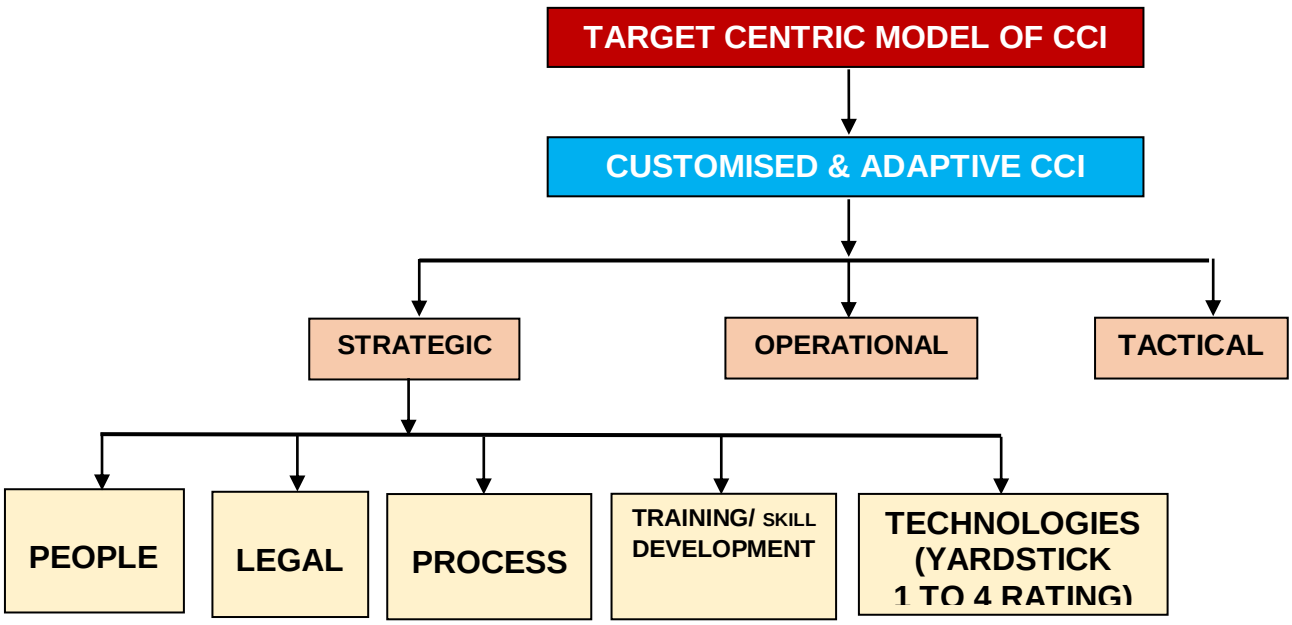

Figure 3: Broad Concept Of CCIM Approach

Offensive Cyber Counterintelligence

Counterintelligence and information assurance are closely linked; they both aim towards upholding information security, reinforcing the confidentiality, integrity and availability of sensitive information. A claim often put forward is that effective counterintelligence (CI) needs to be offensive. Former CIA director of operations James Olson writes that **"CI that is passive and defensive will fail. Our counterintelligence mindset should be relentlessly offensive. We need to go after our counterintelligence adversaries."**[9] CCI is, to an even a higher degree, showing the same patterns, as the focus is heavily set on preventive, and predominantly passive, defensive measures.

The same views were resonated by Allan Dulles, former director of the CIA (1953-1961), who wrote that although the aim of counterintelligence is defensive, its methods are essentially offensive.[10] He concludes that aggressive attacks on the main hostile foreign intelligence services are the most rewarding. Theoretically, this can be explained through military strategist B. H. Liddell Hart's theory of "expanding torrents", which grew out of infiltration tactics introduced during World War I and later evolved to a vital part of the Manoeuvre Warfare theory. In accordance with this line of

thought, offensive counterintelligence can be seen as a battle of resources. Adopting an offensive approach does necessarily need to be aggressive, but is rather concerned with forcing the opponent to react to your actions. In some sense, this can be seen as adding to the “chaos of the battlefield” in order to gain an advantage over the enemy. In the case of CCI deception is a central tool to achieve this goal. If the Foreign Intelligence Security Services (FISS) have to analyze false or irrelevant data (e.g. by being lured to download phony information in a honey trap), or are forced to take defensive measures (e.g. by own systems or assets being targeted by malware by way of infected documents), their resources become tied up and their ability to conduct successful offensive operations is, consequently, limited. A higher level of protection for one’s own organization may thereby be obtained. Being offensive in the CCI process requires a defined and designated target which can be engaged. On the other hand, the previously described complexity of the cyber environment makes an all-out offensive approach taxing. A logical starting point is thus to initially adopt an analysis-driven intelligence process. However, instead of taking defensive actions, the starting point is an analysis of several possible targets – in the case of cyber espionage from an APT, primarily hostile FISS. This includes any foreign organization aimed at attacking or gathering intelligence hurting our national security or interests, intelligence organizations, corporations or organized criminals.

The first step in an analysis-driven approach is to model the opponent – understanding the enemy modus operandi is essential in order to be able to take subsequent offensive action.[11] Once the target is identified, the organization in focus should be selected as the core of the analysis and broken down into manageable pieces.

However, in cyber espionage, the hostile entity gathering information is “blurry” (i.e. hard to classify and identify). Although the analysis-driven approach is needed, the growing amount of available information and the diversity of possible opponents in cyberspace require that it is complemented with data-driven intelligence analysis.

Situational Awareness

The confusion regarding definitions and concepts in relation to cyberspace, that is quite widespread in society in general, also exists within the

intelligence community.[12] A source of this uncertainty is likely mixing the perception of cyberspace as a new intelligence gathering discipline (sometimes called cyber intelligence or cyber collection) with the view of cyberspace as part of Multi domain warfare.

Considering the cyber domain to be a battle arena – countries esp China, North Korea, Iran, Russia US, Israel and NATO have acknowledged the development of several new cyber capabilities in order to achieve desired effects in this operating environment. Being able to attain situational awareness being the key capability in the cyber domain. One of the main differences between cyberspace and the conventional battlespace is the difficulty in understanding when you have been attacked, what actually happened and what the consequences were, and who the attacker was. Having good SA is thus not only a requirement to identify possible cyber threats in a timely manner, it is crucial in order to detect that these threats are targeting one's own resources. Therefore in attaining SA, data-driven intelligence is most useful. By collecting large quantities of data through various cyber sensors, either government-controlled or belonging to the private sector, and processing it with adequate tools and methods, an operational picture can be created in support of cyber operations as well as CCI.

THE ATTRIBUTION PROBLEM

In a cyber espionage scenario, where an APT has managed to acquire valuable or sensitive information by penetrating an organization's cyber defence, the issue of accurate attribution (i.e. finding out who is actually behind the aggression) is a central intelligence challenge due to the anonymous nature of the Internet. A statement that has been highlighted frequently during the last few years is that intelligence failures are usually caused by failures of analysis, and not failures of collection.[13] [14] It is thus commonly not the lack of data per se, but rather the inability to define adequate filters, to make sense of the collected data, and to understand what is important and not, that constitutes the main problem.[15] As data volumes on the Internet move towards the limit of infinity, problems arise in trying to separate signal from noise. The term "big data" is a concept that is getting increasingly relevant in this area. It refers to data sets that are so large and complex that they cannot be processed using readily available database management tools or traditional data processing applications. This

becomes even more relevant when time constraints are present, as is often the case in cyberspace operations or CCI, and puts new demands on processing power, storage, efficient algorithms, and analysis resources.

Detecting Data Leaks

An important part of the process of finding out who is behind a hostile cyber operation, committing cyber espionage, or otherwise engaging in persistent malicious cyber activities, is sorting out what has actually happened and what data that has leaked. Acquiring this knowledge requires that the companies, agencies and organizations that are potential victims of such aggressions are equipped with some sort of security mechanism that monitors information that enters and leaves the computer network. Much of the research during the last decade had been focused on Intrusion Detection Systems (IDS), which offer a measure of protection against cyber threats to information resources. However, since several other attack vectors can be employed, where unauthorized access may be gained through out-of-band channels, e.g. piggybacking on an insecure USB drive, or through attacks initiated by authorized insiders, more attention has recently instead been put on preventing sensitive data from leaving the network, sometimes called extrusion detection or Data Leakage Prevention (DLP). As this method is also useful in detecting that a leak has occurred; even though it may not have been successfully prevented, information about what assets that were targeted and an initial clue about where it went can be attained. The aim of DLP is to take a holistic approach to data protection, including information residing in a computer system (data in use), information on network-attached storage systems (data at rest), and information leaving the organizational boundary via some communications protocol (data in motion).

Data Mining and Process Economics

Data mining, as exemplified through the DLP implementation described above, is only a tool in a larger process. Just providing a tool, while leaving out doctrinal and user aspects, is not enough to provide military utility. A comparison can be made with the introduction of other military tools, such as the machine gun. The impact that the machine gun had on warfare is obvious from a modern perspective. However, this was not the case when it was first introduced. One of the main reasons was that it was considered to

be incompatible with the prevailing doctrine of the time. An offensive tactic was the norm, the machine gun was too heavy for the infantry to carry, and the cavalry had no use of it.[16]

Having access to a new technology or a tool is therefore, by itself, not enough; it also needs to be incorporated into the doctrine and the military system, including user education and acceptance. So although data mining and similar tools have potential to contribute to produce better outcomes within the intelligence sector, they will likely remain useless if they are not adequately incorporated into the military system.

When evaluating the military utility of using data mining tools in intelligence analysis, one must also take process economics into account. Rob Johnston is an anthropologist who spent a year studying the analytic culture of the CIA in the time frame immediately following the events of September 11, 2001. In his book “Analytical culture in the US intelligence community”, Johnston cites an analyst as saying: “We’ve got Bayesian tools, simulations, all kinds of advanced methods, but when am I supposed to do any of that? It takes all my time to keep up with the daily reporting as it is.”[17] There is an apparent compromise between having access to certain tools and having the ability and time to use them efficiently.

The problem can be further exemplified by the above mentioned data leak detection scheme. When used as an input to the cyber attribution process, there may be a non-negligible issue with false positives. There will always be a trade-off between increasing the DR and having a low level of false positives (FP). The relation between actual leaks and detected leaks can be seen in figure 3.

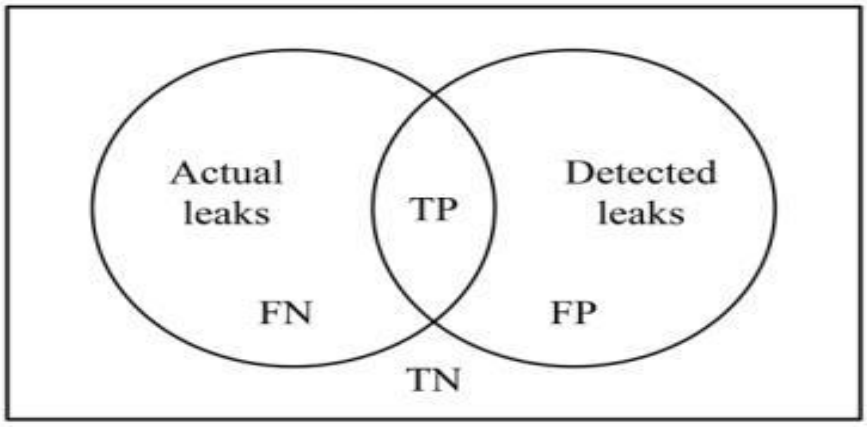

Figure 3. The relation between actual leaks and detected leaks

As the number of detected leaks is related to the required analysis resources, having a low amount of false positives is important. Nevertheless, lowering the amount of false positives will also mean that the detection rate goes down. Finding a suitable balance between detection and analysis capacity is thus key in receiving utility from this tool. As an example, considering the results shown in figure 2, the selected balance between DR and FPR is also related to the size of the total data set and the amount of analytic resources available. Thus, if a FPR of e.g. 1.5 % or 3 % is to be considered acceptable actually depends on the circumstances as described above.

THE CYBER COUNTERINTELLIGENCE ATTRIBUTION PROCESS

Figure 4 presents a generic technical architecture in support of an offensive cyber counterintelligence process. The main goal is to achieve attribution, e.g. finding out who is doing what to our sensitive data. The main parts of this architecture are described below.

The APT attacker, in this case the FISS, uses a network of compromised nodes to perform reconnaissance and to target discovered vulnerabilities in computer resources of victim organizations. Data traffic passing in and out of designated organizations handling sensitive information is processed in order to detect the incidents caused by an APT attack.

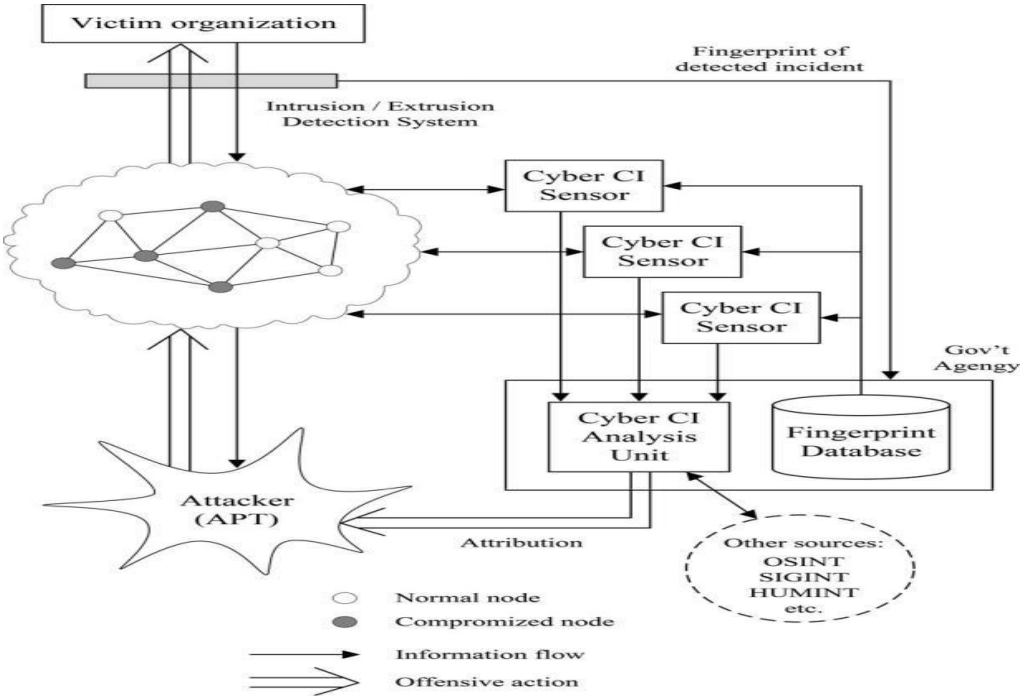

Figure 4. A layout of the offensive CCI attribution process

As discussed above, these incidents could be in the form of either intrusion attempts or data exfiltration attempts, where we will focus on the latter. A DLP algorithm detects data leaks and generated “fingerprints” based on the specific details of the leak. Fingerprints may contain different types of information, such as destination and a hash file of the sensitive information, but should be structured in a standardized format such as Extensible Mark up Language (XML).The fingerprints are collected and forwarded to a fingerprint database hosted by an official entity in charge of the attribution, likely a government agency.

Information from the fingerprint database can then be used by external CCI sensors in order to track the location or path of the leaked information. These sensors can consist of either government controlled sensor nodes monitoring internet traffic, but also of sensors under control of trusted partners – cooperating companies or other external organizations. Some examples are operating system manufacturers, antivirus software companies, Internet service providers, telecommunications companies, and other organizations that may search for matches of the leaked data fingerprints on many internet-connected nodes. If a match is discovered, either that the leaked data is found on a certain node or that it has passed through a node, this information is passed back to the official entity, and is used as input to the CCI analysis unit. Using the information about where the leaks have been seen, in addition to intelligence received from other sources, over time, a puzzle can be completed pointing towards the actual attacker. The validity of the individual pieces of information can of course vary, but by combining the data-driven intelligence with traditional analytic intelligence work, the validity and reliability of the final assessment should be satisfactory.

CONCLUSION

As the cyber environment puts new demands on counterintelligence. A part of the solution might be adopting an offensive target-centric approach. To achieve this, a combination of analysis-driven and data-driven intelligence is needed. The complexity given by the cyber environment calls for cooperation between a diversity of different actors on strategic as well as tactical levels – between government and civilian corporations, different organizations within the intelligence community, analysts and collectors as

well as customers etc. As recently noted by Forbes Magazine in an article on the growing threat of cyber espionage: "[...] unlike traditional crimes, companies cannot just call the cops and let them chase the cyber criminals. Affected organizations play a leading role in every investigation because it is their systems and data that are being stolen or leveraged. The lesson from Mendicant is that we must all come together and collectively fight cybercrime, irrespective of whether the criminal is a rogue hacker or a nation state"[18].The tools discussed in this paper, based on data mining and anomaly detection, show potential of being useful in supporting a collaborative CCI process. However, the utility of these tools is a result of the degree of compatibility with the organizations utilizing them, as well with doctrine and international law. The legal aspects are central in regards to what is allowed in CCI and is an area where large knowledge gaps still remain. Further analysis of the boundary lines between international law and the legal mandate and powers of national police and military authorities is required, as well as studies on how to obtain an acceptable balance between national security intelligence requirements and the legitimate privacy concerns of citizens affected by an increasing degree of government surveillance.

REFERENCES

1. Verizon, "2020 Data Breach Investigations report," 2020 [Online]. Available: http://www.verizonenterprise.com/DBIR/2020/

2. Mandiant Corporation, "APT1: Exposing One of China's Cyber Espionage Units," Feb. 2013 [Online]. Available: http://intelreport. mandiant.com/

3. L. Lam, "Edward Snowden: US government has been hacking Hong Kong and China for years," *South China Morning Post*, 14-Jun-2013.

4. G. Greenwald, "Obama orders US to draw up overseas target list for cyber-attacks," *The Guardian*, 7-Jun-2013.

5. ISO/IEC 27000:2018, "Information technology – Security techniques – Information security management systems – Overview and vocabulary," Second edition, Dec. 2012.

6. N. Perlroth, "Chinese Hackers Infiltrate New York Times Computers," *The New York Times*, 30-Jan-2013.

7. R. Clark, *Intelligence Analysis: A Target-Centric Approach*, 3rd ed. CQ Press, 2009.

8. S. Vogel, “For Intelligence Officers, A Wiki Way to Connect Dots,” *The Washington Post*, 27-Aug- 2009.

9. “FIELD MANUAL 34-60 COUNTERINTELLIGENCE.” Headquarters Department of the Army, 1995.

10. J. M. Olson, “The Ten Commandments of Counterintelligence – A Never-Ending Necessity,” *Stud Intell.*, 2001.

11. A. W. Dulles, *The Craft of Intelligence: America’s Legendary Spy Master on the Fundamentals of Intelligence Gathering for a Free World*, 1st ed. Lyons Press, 2006.

12. M. Herman, *Intelligence Power in Peace and War*, 1st ed. Cambridge University Press, 1996.

13. M. M. Hurley, “For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance,” *Air & Space Power Journal*, Nov.-Dec. 2012.

14. R. Stone, “A Call to Cyber Arms,” *Science*, vol. 339, no. 6123, Mar. 2013.

15. Netherlands Ministry of Defence, “The Defence Cyber Strategy,” Jun. 2012 [Online]. Available: http://www.defensie.nl/english/tasks/ cyber defence/

16. M. Riley, “U.S. Agencies Said to Swap Data With Thousands of Firms,” *Bloomberg*, Jun-15-2013.

17. T. H. Kean et al., *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, 1st ed. W. W. Norton & Company, 2004.

18. L. H. Silberman et al., “The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction,” Unclassified Report to the President of the United States, 31-Mar-2005.

ADDITIONAL REFERENCE

1. R. J. Heuer, *The Psychology of Intelligence Analysis*. Military Bookshop, 2010.

2. K. Burbeck and S. Nadjm-Tehrani, “ADWICE – Anomaly Detection with Real-Time Incremental Clustering,” in *Information Security and Cryptology – ICISC 2004*, C. Park and S. Chee, Eds. Springer Berlin Heidelberg, 2005..

3. A. Lorber, *Misguided Weapons: Technological Failure and Surprise on the Battlefield*, 1st ed. Potomac Books Inc., 2002.

4. D. R. Johnston, *Analytic Culture in the US Intelligence Community: An Ethnographic Study*. Create Space, 2005.

5. J. Westby, "Mandiant Report on Chinese Hackers is Not News But Its Approach Is," *Forbes Magazine*, 20-Feb-2013.

CERTIFICATE

The paper is author's individual scholastic articulation. The author certifies that the article is original in content, unpublished and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

Disclaimer: Views expressed are of the author and do not necessarily reflect the views of CENJOWS.