Towards Offensive Cyber Counterintelligence
Adopting a Target-Centric View on Advanced Persistent Threats

Johan Sigholm
Department of Military Studies
Swedish National Defence College
Stockholm, Sweden
johan.sigholm@fhs.se

Martin Bang
Department of Military Studies
Swedish National Defence College
Stockholm, Sweden
martin.bang@fhs.se

Abstract—Although the traditional strategies for cyber defense in use today are necessary to mitigate broad ranges of common threats, they are not well-suited to protect against a persistent antagonist with access to advanced system exploitation techniques and knowledge of existing but yet undiscovered software vulnerabilities. Addressing the threat caused by such antagonists requires a fast and offensive Cyber-Counterintelligence (CCI) process, and a more efficient inter-organizational information exchange. This paper proposes a framework for offensive CCI based on technical tools and techniques for data mining, anomaly detection, and extensive sharing of cyber threat data. The framework is placed within the distinct context of military intelligence, in order to achieve a holistic, offensive and target-centric view of future CCI. The main contributions offered are (i) a comprehensive process that bridges the gap between the various actors involved in CCI, (ii) an applied technical architecture to support detection and identification of data leaks emanating from cyber espionage, and (iii) deduced intelligence community requirements.

Keywords—cyber; counterintelligence; espionage; anomaly detection; attribution

I. INTRODUCTION

The increasingly pervasive cyber environment of today allows information to flow effortlessly between organizations, systems and people. The integration of physical processes, computation and information exchange has given rise to cyber-physical systems, supporting and facilitating human processes and needs in such areas as transportation, healthcare, disaster response and entertainment. Interconnecting these systems through common networks to the cyber environment provides improved efficiency and functionality, but simultaneously raises new concerns. The growing prevalence of malicious activities in cyberspace makes it a volatile domain, and as major information security vulnerabilities and data breaches make international headlines, addressing the problems of advanced persistent threats, fraud, insider attacks and other cyber-related security incidents are becoming increasingly important for organizations within the public as well as the private sector. As many of the information assets that are sensitive, valuable or critical from a national security perspective are located within the private sector, while the legal mandate to act against antagonists targeting these assets lies within the public sector, an interdependency is created which results in new challenges for the counterintelligence community.

Espionage committed by advanced actors with large resources, leveraging modern information and communications technology, is growing in frequency and scale. These actors are commonly labeled as Advanced Persistent Threats (APT). The recently published (April 2013) 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. [1, p. 21]

The “Mandian APT1 Report” [2] published in February 2013 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
everyday 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 companies and government agencies 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.

However, this practice is slowly changing. The increasing severity of data breaches caused by high-capability adversary entities, with both sufficient resources and intent, has resulted in a more positive attitude towards open sharing of cyber threat data, in order to raise awareness and to learn from collective experience. Recent public disclosures of cyber espionage incidents, such as the one committed against the New York Times in early 2013, [6] have resulted in an increased inter-organizational information exchange to promote common Situational Awareness (SA) in regards to adversary activity, and to help prioritize cyber defense resources. A major benefit of this approach is that one organization’s detection can become another’s prevention.

The challenges described above give rise to new prerequisites for the counterintelligence community in the cyber domain, especially in regards to methodology, tools, information management etc. An open question is thus how the community best should respond to these changes and the challenges that lie ahead.

The rest of this paper is structured as follows. Section II discusses the intelligence process in relation to cyberspace, both as an instrument for intelligence collection and as a battle space. Section III addresses the problem of determining the source of a hostile cyber operation, commonly described as the attribution problem, and discusses data mining and anomaly detection techniques. Section IV proposes a general framework for offensive CCI based on the sharing of cyber threat data gathered through analysis of data leaks, and discusses the requirements of using it. Section V offers some conclusions and suggests possible future work in the area.

II. TARGET-CENTRIC CYBER COUNTERINTELLIGENCE

The specific nature of cyberspace makes assigning responsibility and determining jurisdiction of cyber incident investigations uniquely challenging. The identities of the involved actors are commonly vague at best, and as many organizations across several countries may be affected, variations in language, culture and legal systems may create barriers that hamper response efficiency. Discerning a military aggression from more mundane criminal activities is also non-trivial. When it comes to addressing cyber espionage, a relevant question to ask is if the methodology, processes, and organization prevalent within the intelligence community are suitable for the task.

In the case of the relatively young field of CCI, two of the main challenges are that it is hard to achieve SA, and that the process of attaining positive attribution is perceived as being ineffective. 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 that a heavy focus is put on collection, and that “invisible walls” remain between collectors, analysts and consumers. [7] 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 fulfill within CCI since knowing what to look for demands specific knowledge and a high level of domain expertise in several fields (e.g. technical, legal and cultural). The short time frames of cyberspace also put a higher demand on rapid reaction within the CCI process and on well-functioning inter-organizational collaboration.

An alternative model is given by Robert Clark: the target-centric view of the intelligence process (see figure 1). It is based on the assumption that all stakeholders in the intelligence process (collectors, analysts, processors, 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.

While Clark does not go into any detail in describing how the work within each step of the target-centric process should be conducted, the main point relevant to the case of CCI is that it needs to be a team effort, with close connections between the stakeholders. An example of a

Figure 1. The target-centric view of the intelligence process [7]
A. 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. The specific aim of counterintelligence is to support the intelligence process by countering foreign intelligence and security services (FISS) activities. Counterintelligence is a multidiscipline activity including all forms of action to counter FISS; counter human intelligence (HUMINT), counter signal intelligence (SIGINT) etc.

A claim often put forward is that effective counterintelligence needs to be offensive. Former CIA director of operations James Olson writes that “CI that is passive and defensive will fail. We cannot hunker down in a defensive mode and wait for things to happen. I believe we are spending far too much money on fences, safes, alarms, and other purely defensive measures to protect our secrets. That is not how we have been hurt in recent years. Spies have hurt us. Our counterintelligence mindset should be relentlessly offensive. We need to go after our counterintelligence adversaries.” [10] 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 argument that counterintelligence needs to be offensive is not new. Allan Dulles, former director of the CIA (1953-1961), wrote that although the aim of counterintelligence is defensive, its methods are essentially offensive. [11, p.119] 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 Maneuver Warfare theory. A quick and powerful “torrent” enables own forces to penetrate the enemy’s defense lines and to target his less protected rear units (like a river breaking its banks). It also denies the enemy the ability to fight on a strong, unified front. In the same way, the side that takes the initiative in counterintelligence and makes the first offensive breach greatly increases chances of victory. [12, p. 177]

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 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. [7] 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.

B. 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. [13] 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 a fifth battle arena or domain (besides land, sea, air, and space) in which military operations can be performed. Although these two views are not directly contradicting, and should rather be seen as complementary, the methodological approaches are distinctly different.

Considering the cyber domain to be a battle arena – countries such as China and the Netherlands have recently adopted this view [14][15] – requires the development of several new cyber capabilities in order to achieve desired effects in this operating environment. Being able to attain SA is a key capability in the cyber domain as, analogous to other arenas, decision makers need to have access to a good picture of the current situation, where own and enemy resources are located, the status of important infrastructure assets, how the mission is progressing etc. One of the main differences between cyberspace and the traditional battle arenas 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.

In attaining SA, data-driven intelligence is most likely 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. An indication of that this approach is in current use by the U.S. government has been given by recent (June 2013) media reports. [16]

III. 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 defense, 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. [17][18] 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. [19] 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.

A. 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 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). In this paper we focus on the detection part of DLP, as it will provide an input to the fingerprinting and data sharing function needed in the attribution process. A system for best-effort DLP, an application based on the ADWICE clustering anomaly detector [20], was previously presented in [21]. An evaluation of the architecture gave promising results, as it was shown that a detection rate (DR) of 86 % could be achieved, while limiting the false positive rate (FPR) to 1.5 % (see figure 2). As having access to better intelligence analysis resources allows for handling higher FPRs, even better DRs can be obtained. Allowing for up to 3 % FPR will, with this implementation, yield a 94 % DR.

![Figure 2. Performance of the DLP application previously presented in [21]](image)

B. 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. [22]

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.” [23] 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.

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.

IV. 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. 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 Markup 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.

V. CONCLUSIONS AND FUTURE WORK

In this paper we have discussed the need for an offensive CCI process as a result of the prerequisites of the emerging cyber domain. We have also considered a possible approach of adopting a target-centric view in combination with implementing a technical architecture to support detection and identification of data leaks as a result of cyber espionage.

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 Mandiant is that we must all come together and collectively fight cybercrime, irrespective of whether the criminal is a rogue hacker or a nation state.” [24]

This paper touches on one possible approach to combat advanced persistent treats conducting malicious activities in cyberspace. 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.

ACKNOWLEDGMENT

The research presented in this paper was supported by the Swedish Armed Forces through its program for doctoral studies (Försvarsmaktens doktorandprogram). The authors would also like to acknowledge the support received from the Finnish National Defence University.

REFERENCES