Global Information Assurance Certification Paper

Using COIN Doctrine to Improve Cyber Security Policies

GIAC (GSEC) Gold Certification

Author: Sebastien Godin, sebastien.godin@gmail.com
Advisor: Mohammed Fadzil Haron

Accepted:
(22nd January, 2017)

Abstract

In today's ever-evolving Cyber environment, the "bad guys" seem to prosper, and the "good guys" cannot seem to find a solution to create a proper defensive posture. As the Cyber environment becomes an integral part of society, it is imperative to find a way to increase the global defensive posture in the most efficient way possible. This paper will focus on possible security policies that are easy to implement, are proven, and have a significant impact on an enterprise's security practices and posture. The argument will use field data and firsthand combat experience. Working within the framework of the Cyber environment as an insurgency, applying proven Counterinsurgency policies, there can be a great increase in security and a more efficient Cyber defender. The application of this solution gives the potential for the Cyber defender to have a new set of tools for the Cyber domain that are proven to be useful in the physical domain of a counterinsurgency.

1. Introduction

In today's Cyber security landscape, there are an increasing number of threats coming from old and new sources. The speed, diversity, and frequency of these attacks are creating Cyber security challenges that have never been seen before. Also, the nature and intent of the attacks are changing in that they are becoming more politically and economically motivated and are of a global reach (Verizon, 2016, p.1). There currently is a need to establish Cyber security policies that will help strengthen defense and make the Cyber defender more efficient when reacting to incidents.

The author's current employment is in the military in the Canadian Armed Forces (CAF) with experience in Afghanistan as an Information Operations Officer, where he specialized in Psychological Operations. He was the counterinsurgency (COIN) advisor for the commander on the ground to help him make headway with the local insurgency. The job included: influencing and countering multiple types of events that had a negative impact on coalition forces from kinetic strikes all the way to purely media-based propaganda. These activities taught the author a lot of what COIN is, what works, and, more importantly, what is not functioning; these lessons are applicable when conducting both offensive and defensive operations. Now the author has taken on a new role as part of the CAF's Cyber Forces and has specialized in Cyber defense. In assuming this function, the author has observed many similarities on the conduct of operations in both environments and how successful COIN policy and doctrine apply to Cyber defense activities.

This paper will propose that COIN strategies can be effectively applied to an enterprise's Cyber policies for the purposes of improving Cyber defense[1]. It suggests a shift in thinking about how to proceed with securing an IT environment or Cyber domain, which could apply to entities as small as home networks to the internet as a whole, but the focus will be on medium to large enterprises. The proposed policies are technologically independent, and that will help security professionals and corporate employees achieve a more secure Cyber domain.

[1] For the purposes of this paper, Cyber security is included in Cyber defense.

There are three steps to accomplishing a more secure Cyber defense through the use of COIN strategies. The first part will give clear definitions of insurgency and COIN as they currently exist in doctrine and operational experience that are necessary to the purpose of this argument. The second part will present successful doctrine and policies that work in COIN as they exist in the current operational environment. The third part will translate these definitions, doctrines, and policies for the Cyber domain. This part will also elaborate on why Cyber insurgents have an advantage in the current Cyber environment because of inadequacies toward how the internet, governments, corporations, and individuals operate. Moreover, this research will include examples of policies and how to apply them in the context of a medium to large enterprise, ways of helping the Cyber defender establish more resilient security, and in the event of an incident, recommendations for improved responses.

2. Definitions

To better understand how the goals put forth by this paper can be achieved, the following sections will focus on the definitions that are essential in appreciating why the current state of the Cyber domain is similar to an insurgency. The following definitions will only focus on the military context of insurgency and COIN and will not yet touch how this translates into the Cyber domain. In the third part of the paper will address the importance of having a clear framework that frames real-world COIN doctrine and policy will be useful when translating it into the Cyber domain.

2.1. Insurgency

The difficulty in having a common definition for an insurgency lies in the fact that it is always evolving and adapting in response to each conflict. Nonetheless, there are general trends that help establish when a conflict can be defined as an insurgency. The following interpretations will be used to determine a generalized model for an insurgency:

2.1.1. Local Insurgency

According to the U.S. military doctrine, an insurgency is a subtype of war that is usually internal to a country (The U.S. Army & The U.S. Marine Corps, 2007, p.3). Its

primary focus is typically political in nature with the intent to topple the political power and replace it with the insurgent's power structure. These types of conflicts tend to be lengthy; the usual strategy for the insurgents is to outlast the counterinsurgents by eroding their resources, as a kind of attrition warfare (The U.S. Army & The U.S. Marine Corps, 2007, p.2). According to Kilcullen, to be successful, an insurgency has four key cyclical steps that need to happen. First, there is Infection; where insurgents establish themselves in an area with no law or they may also experience a breakdown in society. Then there is Contagion; the insurgents spread from the contamination area through physical and information operations. Followed by Intervention, the authorities start noticing the insurgents and may take action, both peacefully and violently to quash the insurgency. Finally, rejection is provoked when international forces arrive to help the authorities in the intervention phase and portions of the local population decide to reject the government as they side temporarily with the insurgents (Kilcullen, 2009, pp.35-38).

This cycle (see Figure 1) repeats over time as opportunities for infection are found which enable the insurgency to grow and gain terrain. The longer the counterinsurgents take to counter this cycle, the harder it is to stop. The momentum created by the insurgents makes the actions of the national community seem less significant. This sentiment makes the national community unwelcomed because they are coming in and interrupting the perception of a new "normal life."

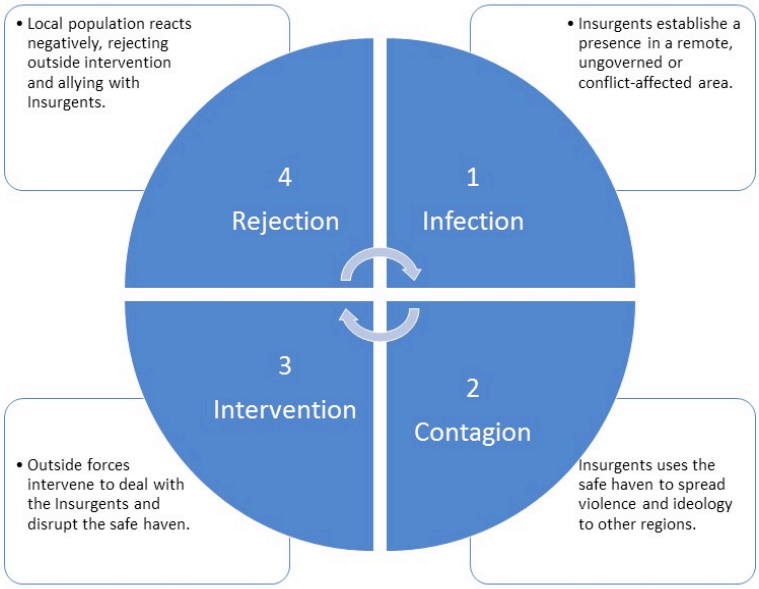

Figure 1 - Insurgent Infection Cycle (Based on Figure 1.1 Kilcullen, 2009, p.35)

Another way of defining how an insurgency evolves is by looking at Mao Zedong's Theory of Protracted War. The theory states that an insurgency will move back and forth through three different phases at any one time. One of these phases is Strategic Defensive, where the authorities have the advantage, and the insurgents focus on survival. The second phase is Strategic Stalemate which happens when there is an equilibrium between the insurgent and government forces, and the insurgent's principal activity is guerrilla tactics. Finally, Strategic Counteroffensive is the last phase and attained when the shift of momentum is towards the insurgents, and there is a move to more conventional war fighting (The U.S. Army & The U.S. Marine Corps, 2007, p.11). Figure 2, as seen below, depicts the characteristics of Mao Zedong's Insurgency Cycle:

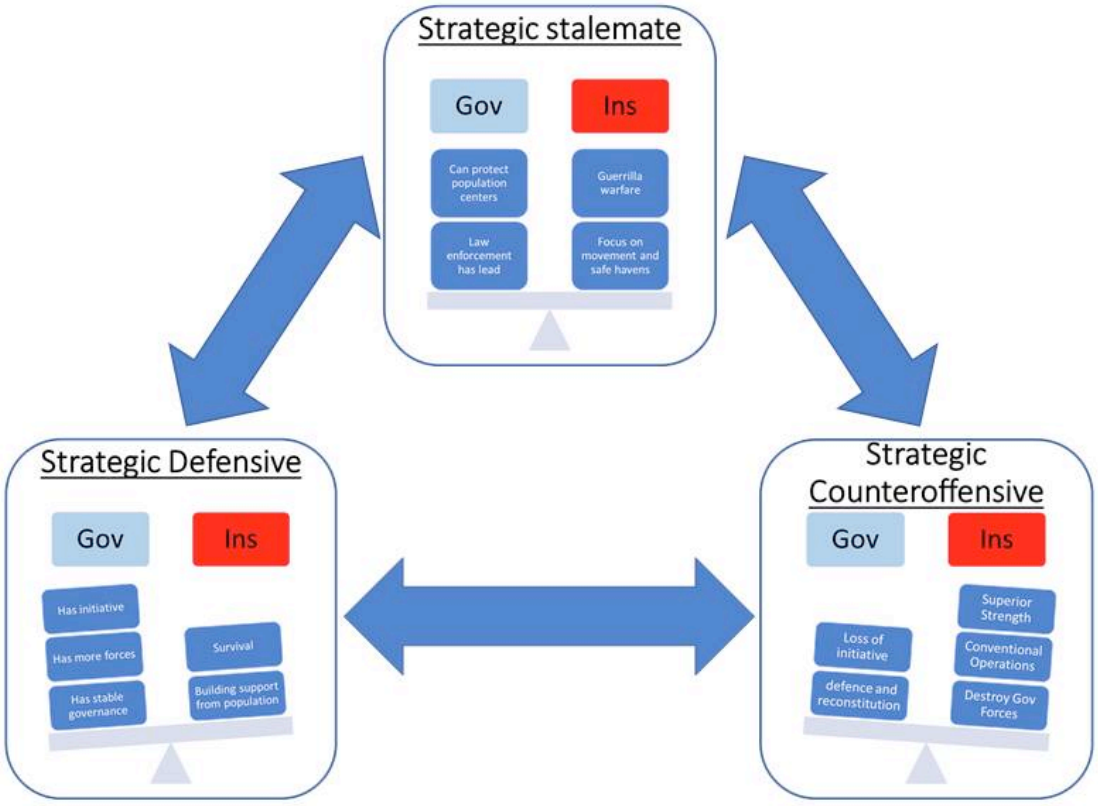

Figure 2 - Mao Zedong Insurgency Cycle

By looking at both Kilcullen's and Mao Zedong's definitions, there can be a few generalizations about how an insurgency behaves and evolves to create a model which will work to define insurgency in the context of this argument. Firstly, to be named an insurgency for the purposes of this paper there must be a conflict between an established entity i.e. government and a counterforce that wants to topple them. Secondly, there are multiples stages based on tipping points where power shifts from balance towards one entity or another. Thirdly, time is a factor; the longer the established power takes to react, the better it is for the insurgents, as this time helps them gain momentum and more resources available to them. These gains assist them in protracting the war and help them to resist attempts from the established power to squash the insurgency. Fourthly, some actors may either be internal to the region, e.g. local population and law enforcement, while other actors may be external to the region, i.e. international forces. Both actors influence the dynamic of the conflict in different measure depending on the stage of the conflict. Moreover, for the insurgent forces, the Center of Gravity, and the key to

winning is the support and acceptance from the local population. This support is key in obtaining resources, information, terrain, and freedom of movement by providing shelter from the established power. This support provides the insurgents with space and time, thus enabling operational freedom.

2.1.2. Global Insurgency

Having a framework of what a local insurgency's main features are is useful, but since the Cyber domain is not usually considered a "local region" but more of a global community, it is helpful to take the established framework of a local insurgency and expand what is needed to make it global. Kilcullen's definition of a global insurgency is useful in this regard and explains how the concepts of a local insurgency can be made applicable to the idea of a global insurgency: "in a globalized insurgency, the insurgents' parallel hierarchy is a *virtual* [*sic*] state: it controls no territory or population but exercises control over distributed systems that, taken together, represent many elements of a traditional state power" (Kilcullen, 2010, p.200). In looking at this definition, the above framework is still valid, only the scale of application changes. Instead of looking at small and mostly homogeneous regions to expand into when conducting a global insurgency, the insurgents must be flexible to adapt their model to regions that are more than likely heterogeneous in nature. This change of scale also means that for the insurgent the command and control structure changes, even if there is a global "head," each region will be autonomous and rely on what the military calls mission command, where the center gives its *intent* but leaves decisions about *execution* to each sub-leader.

In further refining the model for a global insurgency, there are other observable characteristics. Kilcullen states that a global insurgency has eight links between the various local theaters of an insurgency: Ideological, Linguistic and Cultural, Personal History, Family Relationships, Financial, Operational and Planning, Propaganda, and Doctrine, Techniques and procedures (Kilcullen, 2010, pp. 175-181). These links are the basis of trust between each theater and are essential when conducting operations using mission command. Also, by exploiting the similarities that exist within some or all of the links, new insurgents, or even new factions, can quickly be added to the fray or be changed from one region to the other in order to be more operational more quickly.

These links also help the global insurgency in its organization and functioning and according to Kilcullen, makes it behave like an organic system (2010, p.193). This large organic system contains multiple smaller systems that interact together to ensure its survival, i.e. like the human body does. These systems can be considered organic because they share many of the same elements that living systems have. They are social, as they cannot exist in a vacuum and live within a society and need to interact with elements of it to thrive. These smaller systems are energetically open as they accept inputs from their environment and produce outputs that are released back into society. However, these systems are organizationally closed as they have clear boundaries between them and their surroundings. Also, they self-organize depending on the inputs and outputs that each smaller system has by being adaptational and evolutionary. These features are dynamic to ensuring optimal functioning, especially in the event of the sudden death of a lower organism. This composition creates a situation the larger organism that is greater than the sum of the smaller ones, like the human body where each organ cannot do much on its own but works in conjunction with the other organs to create a complex organism. Finally, these systems are nonequilibrium, dissipative structures that cannot self-sustain and will eventually fail if they do not have a constant influx of energy and resources to stay alive (Kilcullen, 2010, pp.193-196). These systems are composed of the following seven elements: Nodes, Links, Boundaries, Subsystems, Boundary Interactions, Inputs, and Outputs (Kilcullen, 2010, pp.196-198). These elements are what define each system's behavior and function within the larger context of the global insurgency. Conducting/performing this analysis on a global scale can be exponentially difficult to do, but once done, will yield benefits in finding targets that have the most value and striking those first.

Lastly, various actors contribute to an insurgency, each with different objectives. There are the insurgents who have a direct claim in the insurgency. There are criminal organizations and opportunists that either take advantage of the chaos or are paid by the insurgents to do illegal activities that can support the insurgents. As previously stated, the local population is an important factor in an insurgent's operational objectives, where portions of them can either directly or indirectly support the insurgent's activities (The U.S. Army & The U.S. Marine Corps, 2007, p.17). The insurgents will focus their effort

on the section of the population that are sympathizers and take advantage of their sympathy to provide direct support to the cause. The insurgents will also expend effort to scare into submission or passivity the rest of the population so that they do not hinder operations.

2.2. COIN

Now that a shared understanding has been reached through the completion of a framework of what constitutes an insurgency, it will now be easier to define what a counterinsurgency is. A practical and complete definition comes from the US military, defining it as the sum of:

> "military, paramilitary, political, economic, psychological, and civic actions taken by a government to defeat insurgency (JP 1-02). […] COIN thus involves the application of national power in the political, military, economic, social, information, and infrastructure fields and disciplines." (The U.S. Army & The U.S. Marine Corps, 2007, p.2)

Therefore, the counterinsurgent is in competition with the insurgent[2] to gain terrain, both physical and "mental."[3] As with the insurgents, the key terrain for the counterinsurgent is the local population. From the counterinsurgent's point of view, the local population can be divided into three categories: those that support the government, those that are neutral (who will neither help or hinder either sides activities), and those that support the insurgents. When taking both the insurgents' and counterinsurgents' points of view, it creates a spectrum on which the local population will shift depending on the phase of conflict and who has the most influence (see Figure 3).

[2] A race condition.
[3] In the Afghanistan theater the term used was "winning the hearts and minds".

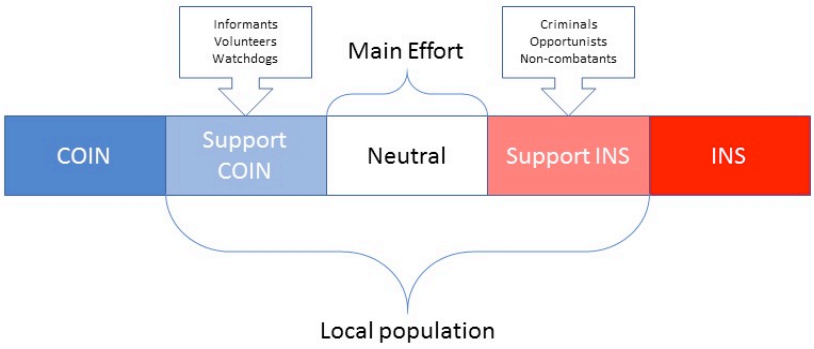

Figure 3 - Local population spectrum

In the application of its power, the government has access to many different entities that divide into a few defined categories; there are the security forces, comprised of government, military, police forces, and Non-Governmental Organisations (NGO) and international assistance, usually in the form of military forces.

Global COIN is the act of countering a global insurgency without primary consideration of national borders, but with a focus on the insurgent links, systems, and elements (Kilcullen, 2010, p.198). All the elements that apply to local COIN shall also apply to global COIN, but there are also other considerations that uniquely belong in global COIN. Also, as much as global insurgency needs to adapt to each region in which it operates, the same holds true for global COIN. As with a global insurgency, there is a unified global intent across all counterinsurgents, where the choice of tactics is left to the commander of each region of operation.

3. Successful COIN Doctrine and Policy

3.1. Successful COIN Doctrine

The rest of the paper will utilize the proposed definition of insurgency and COIN when discussing the actual doctrines and policies currently used by military commanders in theaters such as Afghanistan and Iraq. The focus will be on the military and real-world theories that are successful in fighting insurgencies. Having a clear grasp of these concepts will enable their translation for the Cyber domain in a manner which makes them actionable for non-military organizations.

Author Name, email@address

Before presenting the doctrines and policies, it is important to establish criteria against which they can be evaluated to ensure that they are indeed successful. Kilcullen proposes a method of evaluating success against four criteria or Measures of Effectiveness (MoE): an increase in economic activity, the creation of spontaneous intelligence from the local population, moderate or neutral voices speaking louder and more frequently against the insurgents, and an increase in initiative from the counterinsurgents in initiating actions against the insurgents (2010, pp.225-226). An increase in the first three MoEs is also an indicator that the local population trusts the government and counterinsurgents more to protect them and their way of life against insurgent actions and possible retributions.

This section will discuss doctrine and policy that apply to both local and global COIN. When discussing local COIN, the discussion will focus on actions that their primary purpose is combating a local insurgency but are also applicable against a global insurgency. The reason for choosing these measures, as stated earlier, is that there seems to also be a correlation between global COIN and insurgency and the Cyber domain; this concept will be discussed more thoroughly in the third part.

3.1.1. Local COIN

When fighting a local insurgency, there is no set template; the strategy must adapt and evolve based on the situation and the opponent (Kilcullen, 2010, p.215). One key observation that the author made in Afghanistan is that when conducting a counterinsurgency, cooperation and coordination of effort between all levels of involvement i.e. citizens, the private sector, police, military, Government and international organizations e.g. UN, NATO, Red Cross, are essential for success. To achieve unity of effort, Kilcullen proposes eight best practices which the author can confirm through personal observation. When even one of these practices is not in sync, it can create friction that the insurgents can take advantage of these gaps. All participants must agree on a unified political strategy that will provide a comprehensive approach towards resolving not only military issues but issues of security, economic, social, etc. Participants must commit to seeing the conflict through to the end in one way or another; their level and type of support can change, but their overall commitment cannot. They must focus security efforts on protecting the local population by building a strong

security force through the contribution of resources or mentorship. They must agree to a common method of cueing and synchronizing effects to ensure the effective disruption of systems that the insurgents use to their advantage e.g. safe heaven, borders, and infrastructure. These synchronization efforts are only possible at first and will only be able to survive if there is a close and genuine partnership that survives the inevitable bumps in the road and disagreements (Kilcullen, 2009, p.265). The more people are involved, the harder it is to achieve unity of thought. That is why in Afghanistan there were joint committees that invited multiple governmental departments, law enforcement, military, and even NGOs to reach a consensus to ensure unity of thought and effort.

The most important tool in a counterinsurgency is intelligence (The U.S. Army & The U.S. Marine Corps, 2007, p.79). When looking for sources of intelligence, the analyst must remain open to gather it from all possible sources, even unusual ones. The important task that the analyst must do is the agglomeration, vetting, and analysis of the information. Information can come in many ways and shapes with some being more relevant than others. The main source of intelligence comes directly from the local population; they are the ones that know the terrain and the culture the best (The U.S. Army & The U.S. Marine Corps, 2007, p.80). They can provide better context and observe more minute changes that outsiders cannot. The other important sources of intelligence stem from the partners that are participating in the counterinsurgency and the most efficient way of obtaining this intelligence is by establishing two-way communication channels between all partners. When partners do not share information or intelligence, they are creating gaps in security that the insurgents take advantage of by reusing attacks against those other partners.

A concept that is vital in support of information sharing is that secrecy in defense is a myth. When in defense, the counterinsurgent assumes that the opponent can view and know everything that is being done by probing the defenders and evaluating their responses. An example of this in Afghanistan was when the military was establishing countermeasures against Improvised Explosive Devices (IED). It quickly became apparent that whether an IED strike was successful or not, the insurgents would observe how the counterinsurgents would handle the situation and adapt their tactics in accordance. Then, the defender's best option, like in cryptography, is to have a strong

Author Name, email@address

process that will ensure success even if the opponent knows what and how the defender will handle each situation. This method is how the military established a protocol that was designed to ensure the protection of the forces even if the insurgents were informed of it. The author observed that the number of Canadian casualties due to IED diminished over time. The reason why it was so successful was that the Canadians not only looked at their incidents but also received information from the other nations' incidents and established their protocol based on that information.

The next policy decision that needs to be made to ensure success in a counterinsurgency is the consideration of what the proper ratio of counterinsurgents to the local population should be (The U.S. Army & The U.S. Marine Corps, 2007, p.4). As stated before, when considering how many counterinsurgents are needed to assure security is to focus on how many are necessary to protect the local population. This number is irrelevant of how many insurgents are estimated to be in the area, as they will always focus on the weak points in the defense whether they are one or one thousand. According to US doctrine, an ideal ratio is from 20 to 25 counterinsurgents for every 1000 residents in a defined area of operation (The U.S. Army & The U.S. Marine Corps, 2007, p.23). This ratio ensures that there is a critical mass of counterinsurgents to assure a visible presence to both the local population and the insurgents. The biggest mistake that is seen by commanders when they consider how many personnel they need is the belief that technology can replace boots on the ground. It is imperative in COIN to have a critical mass of ground-based protective forces which are independent of technology. Technology brings more tools, which may be considered to be force multipliers which allow security forces to be more effective and efficient at what they do. Technology enables counterinsurgents to process more information in less time and helps in making better and more timely decisions. In the end, nothing can replace the human presence on the ground in a successful COIN operation.

The last policy that the government has to address is to build trust with the local population so that they appear as a legitimate government that can ensure effective governance (The U.S. Army & The U.S. Marine Corps, 2007, p.37). As stated, the first three MoEs are only able to grow when the local population trusts that the government can guarantee their security and protect them from the insurgents. There are three ways

of achieving this result. First, the counterinsurgents must establish a government that the local population believes represents them. Secondly, the counterinsurgents and government must communicate continuously with the local population to make certain that there is no space for the insurgents to spread misinformation or their agenda. Finally, the government must enable the local population to participate in its security through awareness education and secure tip lines. As was stated earlier, this line of communication is essential to the success of any COIN operation. If the local population cannot trust a legitimate government, it will naturally turn towards what the insurgents propose, no matter how the counterinsurgents destroy or vilify the insurgents.

3.1.2. Global COIN

The above policies are applicable both in a local and a global COIN operation. However, certain policies apply only at the global level (Kilcullen, 2010, p.166). These added policies are needed to address the added complexity of dealing with the global context. Based on the fact that global insurgencies behave like organic systems, Kilcullen proposes a novel way of building strategies for defeating global insurgencies based on complexity theory. This theory is a new way of thinking about COIN systems analysis based on the idea that the systems are organic (Kilcullen, 2010, p.193).

If the main strategy that is derived from complexity theory could be put into one word, it would be *disaggregation*. Insurgencies are composed of multiple systems that have many elements that interact with each other and their environment. As stated, insurgent systems need inputs to survive, as they are not self-sustaining. Therefore, a global COIN strategy should not focus on killing systems but on the links between systems and letting them starve. This strategy is more efficient in the long term and can be far reaching as multiple systems can often depend on one link and therefore, choking off this one link can have a greater repercussion with faster results than just killing each system individually. To find these linchpin links a system's analysis is based on the seven elements of a system and how systems interact with each other. Based on the analysis, the COIN strategy can then use one of the following seven vectors to affect a system: attack the physical nodes or components of a system, interdict the links between systems, disrupt a system's boundaries, suppress boundary interactions, block its inputs

from other systems, deny its outputs to other systems, or a combination of these vectors (Kilcullen, 2010, p.208). How to achieve this can take multiple forms, examples include: disrupting lines of communications both locally and between local and global insurgencies, not allowing sanctuaries by creating a divide between the insurgents and the population, disrupting the flow of resources like personnel, money, or intelligence, and improving local institutional establishments to empower the local population to reject the insurgents (Kilcullen, 2010, p.215). These strategies must be customized, as required, for each theater of operation. The factors that counterinsurgents can consider when customizing their strategy include evaluating demography of the local population, the geography of the region, the length of the insurgency, available resources, etc. Lastly, the strategies or measures taken must not be considered a one-time solution that will work forever; they must be as adaptive and responsive as the insurgents.

These are the main strategies, policies, and doctrines that are currently in use for fighting the insurgencies in Afghanistan, Iraq, and globally that apply to the Cyber domain.

4. Deriving Cyber Defense Policy from COIN Doctrine

4.1. Translating Traditional COIN to the Cyber Domain

As stated earlier, the focus of this paper is on medium to large enterprises. Table 1 will show how the rest of the paper will use previously used terms.

Traditional COIN term	**New Cyber domain term**
Government	The Enterprise's C-suite and director- level staff
Counterinsurgents	Cyber counterinsurgents: Cyber security staff, System administrators, IT support staff e.g. techs and service desk
Insurgents	Cyber insurgents: Individual hackers, Criminal organizations, state-sponsored, hacktivists, and malicious internal threats
Local population	IT infrastructure e.g. routers, servers, desktops,

	etc. Employees
Law enforcement	Appropriate local or federal law enforcement that is responsible for Cybercrime
Partners: International, NGO, etc.	ISP, IT equipment vendors, other enterprises

Table 1

In the proposed model, the enterprise's directing staff has the power to elaborate policies and are responsible for ensuring the proper functioning of the company by protecting its employees and IT infrastructure. It is important to note that what is considered the counterinsurgent force for the corporation includes all IT staff, not just the Cyber security professionals. Including all IT staff makes sense because each staff member has a part in securing and defending the enterprise. Thus, a successful Cyber defense posture includes cooperation from all the IT staff. The enterprise can be considered a local finite area of operation, but they are operating against a global insurgency. Because of this, when considering the proposed policies, they will need to be taken from both local and global COIN to ensure a defensive posture that protects against both types of insurgencies.

To be able to evaluate the success of the proposed policies, doctrines, and strategies, there is a need to assess whether there are improvements that are required. The four COIN MoEs are going to be the basis for the ones that will be used to evaluate the proposed policies for Cyber defense: The economic impact of a Cyber incident on profit and productivity includes: the participation of the local population in the enterprise's Cyber defense, the amount of actionable intelligence that the Cyber defenders have access to, and the amount of time spent enacting proactive measures versus reacting to incidents. Seeing a positive trend in these four MoEs assures an enterprise that the Cyber security actions they are taking are appropriate.

4.2. Links Between an Insurgency and the Cyber Domain

Using the above model and the framework that was established in section 2.1, the connection between an insurgency and the Cyber domain and why Cyber defense

activities are akin to COIN, will be made. According to the established framework, five qualities define a local insurgency plus one to expand to a global insurgency. The first step is to establish is that networks, whether private or public, including the Internet, could be considered a sovereign state[4] with a notional government, i.e. the enterprise leadership, and territory, i.e. the boundary routers. The following six indicators of legitimacy should be used to evaluate the "health" and the threats to the stability of a state (The U.S. Army & The U.S. Marine Corps, 2007, p.38):

1. Ability to provide security for the populace.
2. Selection of leaders at a frequency and in a manner considered just and fair by a substantial majority of the populace.
3. A high level of popular participation in or support for political processes
4. A culturally acceptable level of corruption.
5. A culturally acceptable level and rate of political, economic, and social development.
6. A high level of regime acceptance by major social institutions.

If it is established that an enterprise has the potential to fulfill all six indicators, it can, therefore, fulfill the role of a state. How an enterprise accomplishes this will vary based on the rules that govern the IT domain and its Cyber security posture.

Between the organization and the Cyber insurgents, there is a struggle to maintain control or usurp what is essential to the enterprise: profits. In this case, making the argument that the profits a company determines its competency to govern. Hackers can affect this in many ways by stealing Intellectual Property and selling it to competitors of the enterprise. Hackers can also affect the public's confidence in the company by demeaning their credibility or showing that customer information is not safe; they can diminish productivity by interfering with sales or workers in various ways, these actions satisfy the first criteria of an insurgency. When looking at models for hacking, like Lockheed Martin's kill chain[5], and Incident Handling, like SANS' IH model[6], there are natural tipping points of who has the initiative and there are response mechanisms to try

[4] A **sovereign state** is a political organization with a centralized government that has supreme independent authority over a geographic area (Wikipedia), a nation with its own government, occupying a particular territory (Country, Oxford Dictionary)
[5] http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html
[6] https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

to regain it if lost. The third characteristic is time; the longer the attackers are in the system, the harder it is for the defenders to isolate and expel them from their Cyber domain. The more time the attackers have, the more safe havens they can build and hide within. Then, when an incident is ongoing, both internal and external actors can participate in the resolution efforts like law enforcement, hired Cyber security agencies, insider threats, compromised systems, and other separate attackers, etc. Managing this on both sides can be complex. Finally, the local population is key for both hackers and Cyber defenders to either compromise the IT infrastructure or to protect it. Remembering that in the model, the local population constitutes both employees and IT infrastructure, both need protecting and both can be either willing or unwilling participants in the conflict. From the enterprise's standpoint, these conditions satisfy the five criteria for a local insurgency. The attackers, on the other hand, are operating as in a global insurgency. As previously defined, a global insurgency does not operate in a single operational theater but globally and as such, they must adapt their tactics to each hacking operation. They can simultaneously operate in multiple theaters. Most hacker groups or individuals do not operate in a vacuum; they create links with other groups or individuals that provide other services or support. There is sharing or selling of tools, reselling the hacked information, financial assistance, infrastructure support, etc. Lastly, hackers create links with each other like global insurgents do by using the eight links to gain trust and establish relations. So it can be seen that the enterprise has to conduct COIN operations against an element that behaves both as a local and a global insurgency.

4.3. Cyber Defense Policies for the Enterprise

When an enterprise wants to adopt a COIN mentality to establish a better Cyber defense posture, there is a priority of effort that is followed to ensure success. The first step for an enterprise is to create a strong governance that employees will listen to and trust. To achieve this, all the key leadership in a corporation needs to participate in the Cyber defense governance board. It must be a policy that not only the CIO/CISO will take part in, but also all C-suite executives. As stated in COIN there needs to be a commitment from all participants to push this agenda forward. By having the top-level executives agree and sign off on decisions, this will do a lot to instill in all employees the importance of Cyber defense has to the company. This endorsement also serves as a

visible reminder to the employees that the Cyber threat is real and that the security measures have the backing of all the managers.

The next step in establishing a strong governance model is to have a robust training program. Many other documents cover how to develop a good Cyber awareness program, in a COIN context, the importance resides in the frequency and consistency of the training. In the Canadian military, there is an initial indoctrination training, and there are yearly refreshers that everybody must attend and there are attendance reports sent directly to our Chief of Defence[7], confirming the importance of doing these activities to the employees and managers. It also empowers employees to act according to established security policy and to report incidents with confidence that they are doing the right thing at the right time. The last thing for establishing strong governance is to create a recognition system to reward employees that have acted to prevent incidents or any other action that improves the defense of the company.

The second priority of work for the enterprise is the gathering, processing, and dissemination of actionable intelligence to the company's Cyber counterinsurgents. Going through the arduous task of choosing and creating relationships early on will be beneficial to the enterprise long term. There are multiple sources of information and allies that a company should seek out. External sources include government agencies like the Canadian Cyber Incident Response Center (CCIRC) which is the governmental agency that helps the public sector defend itself through many means. The services offered includes giving industry access to a database of malware seen in wild and sending out monthly or urgent reporting about trends of attacks coming to or conducted on Canadian territory. Then the enterprise should have a policy of establishing a liaison with the law enforcement force that is responsible for Cybercrime. If appropriate and possible, the Cyber governance board should have a seat at the table for a law enforcement liaison to attend. This law enforcement liaison will help with having a coherent direction from the company's direction and will simplify and expedite communications in case of incidents. After that, there needs to be within the service agreement between the enterprise and their ISP covenants on communication lines, information sharing, and responsibilities during times of crisis, including actions to be

[7] Actual spelling of title in Canada

taken to ensure business continuity and disaster recovery. Companies are using more and more cloud services which require a type of service agreement with the cloud service provider.

Lastly, there should be a standing policy to establish information sharing between the enterprise and other firms in the same industry or that use the same IT equipment. Evidently, there are considerations to make for these relations including the protection of Intellectual Property (IP) and keeping competitive advantage even if sharing information of Cyber incidents. There is a case to be made that sharing information on attacks is beneficial economically to both parties[8], prime examples of companies already doing this are the auto and financial industries by creating joint Cyber security centers. The best way of sharing information while sanitizing IP information is to use a standard to exchange information like STIX and TAXII[9]. Internally, like in traditional COIN, the best source of information is from the local population which includes the IT infrastructure and employees. From IT equipment, the gathering and analysis of logs and their behavior are essential in ensuring a proper Cyber security posture and a rapid and efficient Cyber defense reaction. Gathering intelligence from personnel is also critical from reporting malicious emails to social engineering attempts. Teaching reporting mechanisms as part of the security awareness indoctrination and training include: what to report, when to report, and to whom to report. Giving rewards or awards publicly when employees act in accordance with training reinforces these behaviors. An indicator of success sees an increase in the participation of the employees which are usually quiet or non-participative become part of the solution and create momentum and excitement for Cyber security. The last decision regarding intelligence collection is the implementation of a system that will gather, organize, collate, and do an initial analysis of all the collected information. This system can take the form of an intelligence cell or a SIEM. However, the technology is irrelevant as long as there is a systematic approach with a feedback mechanism to the creation of intelligence that will enable the Cyber security

[8] The Author has written an unpublished paper for a US military Cyber security course using game theory and Superrationality to prove that companies that share information have an economic advantage over not sharing.
[9] https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity, pulled 12 Jan 17

team to prevent an intrusion, detect an intrusion, find the intruders, and respond to protect the system faster and with more precision.

The next policy decision is the size of Cyber counterinsurgent force that an enterprise needs to ensure a strong defense that can both prevent and respond effectively. Remembering that the ratio that COIN uses is based on the local population and not the number of insurgents, the same logic should apply. The author would suggest using the same ratio of 20-25 per 1000 local population based on his experience of doing Cyber defense for the CAF. When looking at an enterprise with 10000 employees and 15000 pieces of IT equipment giving the company a total local population of 25000, there should be between 500 and 625 Cyber counterinsurgents. This number might seem high, but remember that this figure includes system administrators, service desk personnel, technicians, and Cyber security experts. Representing only 2 to 2.5% of an enterprise's employees is not an unreasonable workforce to dedicate to protecting an operational business that needs to ensure that the IT domain does not hinder productiveness. It is also important to stress that newer defense technology does not replace trained personnel, it only enables them to be more efficient.

As previously stated, an enterprise acts as a local COIN operation against a global insurgency and an enterprise cannot be expected to end all malicious activity on the internet. However, there are actions that a company can take to ensure they are not part of the problem. When trying to apply the principle of *disaggregation,* the main effort should focus on severing the links between the attackers' systems; for an enterprise, this means making certain of two measures. The first one is to make certain that there is not a link between the insurgent's systems by acting as a node or a transit point, the previously discussed policies will help ensure that the enterprise's Cyber domain does not become a haven for the malicious actors. The second is doing a supply chain analysis to ensure its integrity, enforcing this through contracting. The Department of National Defence[10] (DND) has adopted a contracting policy that states that companies must maintain a minimum of security as per the government's IT security policies, that the corporation reports any breaches, and to let the government audit the company's security posture.

[10] Government of Canada organisation

These measures will at least ensure that the enterprise does not provide shelter or resources to malicious actors and forces them to these commodities elsewhere.

5. Conclusion

The policies, doctrine, and strategies for Cyber defense proposed in section 4 will help an enterprise, based on tested COIN principles, have a stronger security posture. Adopting these measures will ensure that the four core principles of conducting a COIN operation are respected. This can be done, firstly, by making sure that the enterprise has a strong governance model that will promote participation and compliance from employees and managers. The coordination and collaboration between the principal figures in the business towards a common approach and set of goals will help solidify the Cyber governance boards role and standing. Secondly, the sharing of intelligence both horizontally with partners and vertically with the local population of the enterprise helps increase its security posture of the Cyber domain and decreases the response time of the Cyber defenders. Thirdly, by having a proper ratio of Cyber defenders to the local population is critical to give and maintain a sense of security and to capitalize on the gathered intelligence. Finally, by using complexity theory's principles of systems analysis, the Cyber defender can focus on defending or targeting the points between systems that are crucial to survival with higher efficiency and with less trial and error. These measures fulfill the MoEs established at the beginning of para 4 and will over time make the total cost of ownership of the Cyber defense program be less than reacting and managing breaches. Moreover, although the focus of this paper was for medium to large enterprises, the advantage of this new way of thinking is that it is scalable from the little guy all the way up to international entities.

Author Name, email@address

6. References

Carr, Jeffrey. (2011). *Inside cyber warfare*. (2 ed.). Sebastopol: O'Reilly Media, Inc.

Coll, Steve. (2005). *Ghost wars, the secret history of the CIA, Afghanistan, and Bin Laden, from the Soviet invasion to September 10, 2001*. Penguin.

Kilcullen, David. (2009). *The accidental guerrilla*. Oxford: Oxford University Press.

Kilcullen, David. (2010). *Counterinsurgency*. New York: Oxford University Press.

Reed, John. (24/04/2013). The takeaway from Verizon's cyber security report: Cybercrime is way too easy. *Foreign Policy*. Retrieved 20/06/2013, from http://killerapps.foreignpolicy.com/posts/2013/04/24/the_takeaway_from_verizons_cyber_security_report_cybercrime_is_way_too_easy.

Roberston, Joran. (25/04/2013). The Latest Cyber Warfare Weapon: A Hacked Twitter Account. *Bloomberg*. Retrieved 20/06/2013, from http://www.bloomberg.com/news/2013-04-24/the-latest-cyber-warfare-weapon-a-hacked-twitter-account.html.

Stevenson, Alastair. (25/04/2013). Infosec 2013: Governments will fall if cyber attackers succeed, warns MoD. *V3-co-uk*. Retrieved 20/06/2013, from http://www.v3.co.uk/v3-uk/news/2264063/infosec-2013-governments-will-fall-if-cyber-attackers-succeed-warns-mod.

The U.S. Army & The U.S. Marine Corps (2007). *The U.S. Army and Marine Corps counterinsurgency field manual, U.S. Army field manual no. 3-24: Marine Corps warfighting publication no. 3-33.5*. University Of Chicago Press.

Verizon (2016). *2016 Data Breach Investigations Report*, Retrieved December 25, 2016.

Last Updated: June 24th, 2018

Upcoming Training

SANS Cyber Defence Canberra 2018	Canberra, Australia	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Vancouver 2018	Vancouver, BC	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	Live Event
Community SANS Nashville SEC401	Nashville, TN	Jun 25, 2018 - Jun 30, 2018	Community SANS
SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, Singapore	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
SANSFIRE 2018 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 16, 2018 - Jul 21, 2018	vLive
Mentor Session - SEC401	Jacksonville, FL	Jul 17, 2018 - Aug 28, 2018	Mentor
Community SANS Annapolis Junction SEC401	Annapolis Junction, MD	Jul 23, 2018 - Jul 28, 2018	Community SANS
SANS Riyadh July 2018	Riyadh, Kingdom Of Saudi Arabia	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PA	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS Boston Summer 2018	Boston, MA	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, Australia	Aug 06, 2018 - Aug 25, 2018	Live Event
San Antonio 2018 - SEC401: Security Essentials Bootcamp Style	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, India	Aug 06, 2018 - Aug 11, 2018	Live Event
Mentor Session - SEC401	Ankara, Turkey	Aug 08, 2018 - Oct 03, 2018	Mentor
Northern Virginia- Alexandria 2018 - SEC401: Security Essentials Bootcamp Style	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	vLive
SANS Northern Virginia- Alexandria 2018	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS New York City Summer 2018	New York City, NY	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VA	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS Chicago 2018	Chicago, IL	Aug 20, 2018 - Aug 25, 2018	Live Event
Mentor Session AW - SEC401	Raleigh, NC	Aug 22, 2018 - Aug 29, 2018	Mentor
SANS San Francisco Summer 2018	San Francisco, CA	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, Japan	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, Netherlands	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FL	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MD	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201809,	Sep 11, 2018 - Oct 18, 2018	vLive
SANS Munich September 2018	Munich, Germany	Sep 16, 2018 - Sep 22, 2018	Live Event