2014 6th International Conference on Cyber Conflict
P.Brangetto, M.Maybaum, J.Stinissen (Eds.)
2014 © NATO CCD COE Publications, Tallinn

Cyber Fratricide

Dr. Samuel Liles
Purdue Cyber Forensics Laboratory
Purdue University
West Lafayette, USA
sliles@purdue.edu

Jacob Kambic
Purdue Cyber Forensics Laboratory
Purdue University
West Lafayette, USA

Abstract: The United States military is currently one of the most powerful forces on the face of the planet. It achieves this in part through a high level of organization and interoperability borne through the use of the continental staffing system by the U.S. and many of its NATO allies. This system is meant to separate functions and facilitate efficient flow of information to those who need to make command decisions. While it has proven effective in prior conflicts, it has become outmoded in the information age, instead stifling necessary coordination and collaboration through isolation and insulation between roles. This paper contends that the constructs used by the continental staffing system, like that of area of operation, and rigid segregation of duty through tradition, expose a seam in the system which leads to unanticipated and negative consequences on friendly forces referred to as “cyber fratricide.” Cyber Fratricide may be considered the unintentional impedance or interference between operational/tactical elements of friendly forces in the cyber realm involving the compromise or liquidation of assets, information, or capabilities of those forces. This is especially important when considering active or transactional hostilities by multiple actors. This is especially true in the case of shooting back in cyber space or active defence. By observing the most common possible forms of cyber fratricide and their enabling factors, conclusions may be drawn on possible mitigations through technical controls and reengineering of the continental staffing system to reduce cyber fratricide in active defence. This paper is a discussion of one issue in active defence and is not meant to be a complete treatise on the topic.

Keywords: *active defense, cyber fratricide, risk tolerance*

1. INTRODUCTION

The United States Military has proven itself to be one of the most capable forces on the face of the planet. It maintains this capability, in part, through a high degree of organization and specialization. One driving component of this organization is the use of the continental staff system, which enumerates functional areas of expertise. The continental staff system, used by NATO countries, assigns numbers to these areas of expertise. For instance, the intelligence officer is identified by the number 2, the operations officer by 3, and the communications officer by the number 6. The continental staff system is meant to separate functions and facilitate the efficient flow of information to those who need it to make command decisions. Historically, the continental staff system has provided an effective method of structuring this information flow for maximum benefit.

We have known for quite some time that this organizational scheme is proving to be less effective as military operations both expand into and rely more heavily upon the cyber domain (Arquilla, 1993). Closer observation of the continental staff system reveals that its rigidity and compartmentalization, formerly benefits of that system, can, in the current information age, lead to unanticipated and negative consequences. This paper considers these consequences, and proposes that "cyber fratricide" is a real threat that needs to be addressed. Cyber fratricide is the unintentional impedance or interference between operational/tactical elements of friendly forces in the cyber realm, and can involve compromise or liquidation of assets, information, or capabilities. In what follows, the causes of cyber fratricide are discussed, examples of how cyber fratricide might occur are examined, and finally, strategies to avoid cyber fratricide are explored.

Currently, staff roles are assigned to specializations that are in likely conflict with their original purpose, which can cause strains on the aforementioned organizational structures. Additionally, achieving situational awareness requires the intelligence, operations, and communications officers to function together when dealing with cyber assets, yet, by design, several of the roles are mutually exclusive and constrained with respect to their visibility and interaction with cyber assets. In order to fully qualify these statements and explore the issues in further depth, some context is required for both the original functional roles and their typical purview (in terms of area of operation).

Each unit or military command has an area of operation. This area can be as small as a few hundred square meters at the squad level or multiple continents at the combatant commander level (the highest division of responsibility/mission in the US armed forces). The discussion that follows will focus on the battalion through combatant commander spectrum, and does so mostly interchangeably. These generalizations are crude but intentional, and the patterns being addressed here should hold up fairly well across this spectrum. Area of operation will play a significant role in one aspect of the later discussion on cyber fratricide through active defence.

Three officer positions in the continental staff system are most pertinent to analyse the issue of cyber fratricide and will now be discussed in greater detail: the intelligence officer (2), the operations officer (3), and the information communication technology (ICT) officer (6) (Joint Chiefs of Staff 1993, II-4).

Traditionally, the intelligence officer (2) has been tasked with collection and stewardship of knowledge about enemy assets (Joint Chiefs of Staff 2007b, III-14). In the cyber domain, these assets come in forms like critical infrastructures, communication nodes, components of current intelligence collection methods, and accesses created to the other (cyber) assets mentioned so far. The intelligence officer is supposed to keep the knowledge of tools, techniques, and procedures used in the intelligence collection process secret, divulging only the intelligence products dictated by the mission and circumstances that arise during its execution; however, depending on the operational level of an intelligence officer, he or she may not actually be directly creating or implementing accesses for collection, but rather is only a consumer of intelligence themselves, engaging a party external to the mission to create/activate an access to collect/observe from at their behest. In this case, the intelligence officer may have obtained relevant operational intelligence to filter and disseminate, but have no knowledge of its provenance nor the mechanism by which it was obtained. This causes problems because the intelligence officer has caused the creation, through external mechanisms, of an access to an enemy asset for observation. Unlike other forms of access or observation, the cyber domain is transactional. This means that accesses created at the behest of the intelligence officer for his observation and action in cyberspace may allow an adversary observation and action back into the intelligence officer's organization. It is worth noting that the intelligence officer (2) will authorize or be the user of accesses created through active exploitation of information assets.

The operations officer (3) is the person who will act upon this intelligence, and operationalize the plans of the commander, ensuring the resources are ready as planned by the strategies and plans officer (5, not previously discussed)(Joint Chiefs of Staff 2011, II-1). This officer is motivated to achieve mission objectives and overcome any obstacle to the success of the mission. The operations officer will confer with his or her other staff officers when moving a plan forward to ascertain that there are no issues or concerns prior to moving past the line of departure, where the line of departure is the point at which the possibility of contact with the adversary will become material. It is imperative that this staff officer has as much information as possible upon which to build/implement the organizational strategy—coordination and collaboration are specific concerns in this capacity.

The information and communication technology officer (6) keeps communications available and manages the infrastructures required to provide the commander with command and control. This officer will coordinate which frequencies are used in a battle and how much bandwidth is available or provisioned to entities in the area of operation (Joint Chiefs of Staff 2011, D-3). In the past, the ICT officer was considered to be primarily a support role along with the logistics officer (4), but this officer is rapidly transitioning to a role as a cyber operator. Here-in lies the problem. This transition is the fulcrum upon which a series of past policy decisions start to bend towards a breaking point: asking an ICT officer, primarily trained in facilitating communication, to project power into enemy held positions exposes a fundamental flaw and observable cascading policy failure in the current implementation of the continental staff system.

When the commander wants to proceed with an operation in cyberspace he or she may want to achieve a myriad of possible goals: blind the enemy for a few moments, deny them access to an asset in a combined arms fire, create a point of societal disruption, or deny safe haven to a command and control system, as a few examples. Regardless of the request, the current process of information flow would necessitate obtaining a doctrine or planning document from the strategies and plans officer, passing it to the operations officer, who in turn would make changes and or additions to the plan, obtaining any required information that he or she can from the intelligence officer, and finally, coordinating command and control communications through the ICT officer (Joint Chiefs of Staff 2006, I-14). Despite the apparent utility and simplicity of this information flow, which is dictated by the continental staff system and its processes, the reality is that this is not how the flow actually occurs for operations in cyberspace.

2. CYBER FRATRICIDE

Instead, in this realm, the traditional flow of communications breaks down and this breakdown can in turn lead to cyber fratricide. The cyber fratricide occurs when agents in one friendly domain negatively impact the actions of agents in another friendly domain because of the blurry boundaries inherent to cyber conflict. Several forms of cyber fratricide are possible, depending on the configuration of agents involved and their associations with one another.

These associations are more readily explained by dividing assets into different groupings. When discussing any conflict domain, assets are conventionally color-coded, with red indicating enemy assets, green indicating neutral assets, and blue indicating friendly assets. For our purposes, blue can be further separated into intelligence, operational, and domestic assets.

This division allows the identification of three forms of cyber fratricide. The first is blue operational entity on blue intelligence entity because these two entities are specifically not in close, bidirectional communication. The second is blue operational entity on green due to close association with a red information asset. Finally, a third form of cyber fratricide occurs due to ineffectual use of the area of operation paradigm and involves blue military operations acting on blue domestic assets in contravention of national laws and norms, possibly in violation of the Posse Comitatus Act (a limitation on the use of military personnel against US civilian population). These three forms of cyber fratricide are further explored in what follows.

The cyber domain is currently held to be within the purview of the communications officer (Joint Chiefs of Staff 2011, II-1). This officer's mission is primarily defensive in the context of cyber situational awareness. In order to carry out a cyber-fires mission, however, communications officers may be called upon to execute/conduct offensive activities (Computer Network Attack) that transit a "blue" network. Such a situation involves the first form of cyber fratricide— it is possible for any munitions, regardless of domain, to injure friendly troops thus creating blue on blue fratricide. In the case of the communications officer this could degrade, disrupt, or even destroy his ability to provide his primary (defensive) functional capacity. If asked to facilitate or attempt a cyber-fires mission from a blue network, the communications officer is being metaphorically asked to shoot at his foot and hopes he misses. In addition to possibly infecting, attacking, or degrading service to friendly nodes within the blue network during execution of the attack, he or she may incidentally grant a red entity access to the network or destroy blue assets in the course of his or her original defensive duties. As an example, if an officer asked to secure the network found an access that he or she did not have prior knowledge of (but was created or requested by an intelligence officer), they might reflexively apply security controls to the connection and destroy or disclose the access. In such a scenario, the ICT officer was not in direct, bidirectional communication with the intelligence officer who, following protocol, did not disclose the means used to collect the operational intelligence, or possibly was not aware of exactly how the access was created/initiated. These examples highlight the first form of cyber fratricide by a blue operational entity on a blue intelligence entity due to the breakdown in communications and information flow spurred by the compartmentalization of the continental staff system in its current implementation.

The operations officer has yet another problem: the concept of area of operation itself is inherently flawed and outmoded in terms of a "cyber" fires mission. For example, an information asset may be accessed and leveraged by a terrorist cell in Afghanistan that is proxied through Russia by way of a Chinese Internet Service Provider with the operational asset physically located somewhere in Atlanta, Georgia. In such a case, the functional area of operation might realistically span all of the combatant commands combined. Acting on the asset would realistically be a blue operational entity acting on a blue civilian asset, currently controlled or accessed by a red operational entity transiting a green network. Further exacerbating the matter is that should the targeted red asset instead be within the locale of the red entity, Afghanistan in this case, it may still simultaneously be a subset of a green asset. That is to say that the red asset might be purchased from and managed by a third, green party that is unaware of its use for nefarious purposes or it may exist within an allied or neutral sovereignty. Considering an operation against the red entity illuminates a second form of cyber fratricide – the incidental targeting of a green entity due to its close association with a red asset.

Another consideration is that, in the current United States military paradigm, the cyber mission is inextricably linked to the intelligence function. A testament to this is the close association and collaboration between United States Cyber Command and the National Security Agency. However, the intelligence officer may only have a vantage point over (or able to develop intelligence products for) missions that are in his or her area of operation. Then consider that if an organization outside the scope of such an operation, like the U.S Cyber Command, is creating the accesses or is facilitating intelligence collection they may not, and likely should not, be communicating that activity. Additionally, if another intelligence organization is involved in the creation of access to a red asset, said organization may not even be in the target approval process of the asset for the mission's area of operation and thus unaware of intentions of the designated combatant commander. Finally, consider again the compromising position of the communications officer who, in the course of his primary (defensive) duties in these situations, is thus placed at odds with the operations officer, the intelligence officer, and his own commander when setting up a "cyber" fires mission.

3. EXAMPLES

To help illustrate these scenarios of cyber fratricide in a more concrete manner, a vignette of a mock operation utilizing cyber capabilities coupled with real world examples will now be examined. Envision that a commander wants to create a specific effect. Perhaps the commander has a mission to arrest or detain a high value red adversary within his or her area of operation. It is determined that, for a combat team to enter the area without using extensive force, a disruption of the traffic control system of a city is needed. The mission summary, then, is that blue cyber forces will disrupt, degrade, or destroy a city traffic control system. The expected effect is traffic congestion slowing response of red forces to the incursion of blue ground forces.

The planning and operations officers have evaluated several possible scenarios and outcomes of each scenario, and green-light the operation.

A kinetic attack on the traffic control system might alert red forces to a pending offensive, but a technical disruption might be interpreted by red command as incidental, and slow the realization of the true nature of the outage. In this case, since blue knows the traffic snarl will occur, blue air assets will provide reconnaissance of egress points. Blue ground assets will acquire and detain the red leader while making egress from red territory. It is expected that a small team of blue ground assets will not be detected until contact with the red leader, and that red response after realizing the nature of the attack will be constrained by the outage. Thus, a small operation will have larger strategic consequences.

A traffic control system is a real time system that uses sensory input to create a specific set of behaviours at the light-signal end. In many cities these kinds of signal computers are centrally controlled. The red asset of the traffic control lights are fully in the area of operation. Reconnaissance of these cyber assets by intelligence entities of blue confirms that the control systems themselves are fully in the area of operation. Unfortunately, the intelligence officers have not been apprised of the nature of the mission due to its classification. The intelligence officers therefore did not consider that a green entity has been outsourced to monitor traffic control systems in this area of operation. Furthermore, that green commercial entity is operating out of a control center positioned in the U.S. The outsourcing of such tasks, even between hostile adversaries, is commonplace. This is an example of the principle of globalization at work, and is the first unforeseen complication in the operation.

The next command decision is which blue cyber operators will engage in the mission within the area of responsibility. This is actually a tenuous point that should be considered carefully. In current conceptions, the entirety of cyberspace is often (mistakenly) considered to be a valid and available attack source. The question of whether the blue cyber operators should be located in the continental United States or in the area of responsibility of the commander does not have a simple answer. If the attack is launched from the United States itself, then there is no legal construct to keep the adversary from returning fire. On the other hand, if it is launched from the current area of responsibility of the commander, and then fires are directed at the United States, inadvertently/incidentally in the case of targeting the green control center, it could easily be construed as "targeting blue civilian infrastructures" and therefore be classified as a war crime. This is a thorny and convoluted legal problem.

Coordinating fires in cyber can also be a problem. Since situational awareness can be degraded by the compartmentalized command staff structure, it should come as no surprise that the operational capacity in cyber can also degraded. If the fires mission is put on the communications officer then a host of legal and policy implications ensue. In the narrative followed thus far, the concept of injecting the Department of Defense network (DISN) with a virus or cyber weapon for delivery to a civilian system is tantamount to treason—even in combat. So if the blue operator uses the cyber weapon across their own network, there are grave policy consequences looming.

The communication officer may also be providing services to the intelligence group through a coordination point or staff member. This becomes relevant when you think about the intelligence information assets that the communications officer may not even know exist. Yet it may be the intelligence officer who prepares the red information asset for exploitation and provisions separate networks for just this occasion. As such, it will likely be the intelligence officer who actually disables the red information asset. However, this is contrary to that staff officer's role and the person "pushing the button," metaphorically, should be the operations officer. Such routine deviations also point to a systemic issue in the application of tradition organizational constructs (especially the current continental staff system) to the cyber domain. This rather involved and murky example is just what creates the danger of cyber fratricide under the current concept of operations and staff structure.

In addition to the fictional example of a U.S. operation that was just presented, we can also observe documented situations abroad that underscore key elements of cyber fratricide discussed. In 2008, Pakistan engaged in what was described as an act of "information provincialism" when it decided to censor youtube.com ostensibly due to the potential of certain content to foment civil unrest (Stone, 2008). This operation however went awry and in the implementation process, Pakistan configured the externally facing BGP (Border Gateway Protocol) interface to black-hole traffic destined for youtube.com, this configuration then being propagated to the Internet at large (Stone, 2008). The result was youtube.com being "black-holed" across the world, producing an effect which accomplished their mission set but also created an international diplomatic incident.

This last portion is crucial to the incident's significance in the vein of cyber fratricide: a technical control was implemented, to effect, which also had far reaching, negative consequences throughout the organization and incidentally its allies. It also emphasizes the difficulty in controlling aspects of the area of operation within cyber from a technical perspective. Had the operation enjoyed a more tempered success and been effective only within its intended area of operation, the Pakistani nationalized network infrastructure, there were still possibly unforeseen issues. Completely screening an entire source of information and information distribution, particularly social media, sincerely degrades situational awareness. If they wanted to allow select elements within the governmental institution to monitor Youtube® at that point, they would have to create an access, which could then undermine the control put in place and complicate the operation. This control also fails largely because of the technical countermeasures not taken into account during the planning phase or evaluated during the implementation (or "Action") portion of the operation (for instance, the use of proxy hosts).

Another more direct example of cyber fratricide in the context of military operations can be found in the alleged Chinese cyber espionage campaigns described in Mandiant's "APT1" report. The premise of the report is that Chinese operatives under direct supervision of the People's Liberation Army (PLA) have been infiltrating private sector entities of other nations, notably the US, and extracting voluminous amounts of secrets/classified information. One of the reasons that these activities were detectable and directly attributable to the PLA was the separate provisioning of attack networks. While generally this is a standard practice in offensive operations, in this particular instance it was incredibly anomalous due to China's otherwise strict control of information flow in and out of the country, sometimes colloquially referred to as “the Great Firewall of China.” Because of the tight controls implemented by this censoring group, the attack infrastructure for the APT group became very apparent, and Mandiant was able to identify that “of the 614 distinct IP addresses used […] 613 (99.8%) were registered to one of four Shanghai net blocks” (Mandiant, 2013, p 4). This is an excellent example of cyber fratricide, where the activities of one blue operational unit degrades or destroys the assets or operational capacity of another blue group.

The vignette and events highlighted only scratch the surface of what is possible—as they demonstrate, the construct used for area of operation, and the information flow of the continental staff system, can have serious impacts that may lead to cyber fratricide. Additionally, other scenarios can be envisioned in which cyber fratricide could lead to a host of issues such as unintended red access to blue networks, or information exposure to red about blue assets, logistics, relationships, or personnel. Gravely, these situations could lead to the degradation or complete failure of the operation after leaving the line of departure, possibly at the cost of life to teams on the ground. This can also reverberate at scopes well beyond of the operation, affecting the entire organization.

4. CONCLUDING REMARKS AND POSSIBLE SOLUTIONS

In order to address the issue of cyber fratricide, changes to both the processes and organizational structures of the continental staff system are necessary and they concept of Area of Operations are neccesary. This can possibly be accomplished through the introduction of injection points, the use of additional technical controls, and the fixing of expectation gaps with respect to mutually exclusive objectives of specific staff positions within the continental staff system. Having a high level overview of the cyber targeting team, while knowing the specific staff issues, will allow us to engage in good situational awareness and decrease cyber fratricide.

For better information convergence during the operational planning phases, injection points can be created that are similar to those assessment points currently in place for the targeting and planning phases. In this way, a feedback loop can be established as the operation commences to improve agility and situational awareness thus reducing the possibility of cyber fratricide, particularly when also feeding in assessments from prior information operations. This can be complimented by redefining of duties for the established staff positions to meet the current need as we continue to expand operations in the cyber realm.

An ICT officer is charged by law and necessity to maintain the communications’ fidelity, sanity, and resilience at all times. This officer is not a fires officer, but true to its intended purpose, is supporting an infrastructure necessary to the operations. As such, he or she simply cannot be used to project power into enemy held positions without the threat of degradation or compromise to that internal infrastructure. Therefore, a separate entity needs to carry out the offensive role in cyber. Equally, however, the operations officer cannot use their own network connections to conduct attacks. This compromises the position of the ICT officer, because, as noted previously, the transactional nature of cyber means that doing so can create an access back into the attacking network by which the adversary may respond. Uniquely, this means that the overall effects can be detrimental beyond the scope of the fires mission: if you fly an airplane into combat from an aircraft carrier, it rarely has a significant impact on the carrier, yet in cyber, you can have issues and impact across the entire organization. There are several architectural and doctrinal changes that can help mitigate this risk of cyber fratricide and can be facilitated by technical solutions.

Architecturally, developing a command and control (C2) apparatus that is capable of taking into account the health of the C2 apparatus itself and the segregation of this apparatus from supporting technical infrastructure (with the understanding that full segregation is not truly possible) would be a vast improvement defensively. In addition to this seperation, there should also be a convergence in the support infrastructure through the implementation of coordination and decision support systems that will allow increased communication earlier on in the process between strategies and plans officers and ICT officers, and the introduction of both targeting and threat reduction tools such as the Theater Battle Management Core Systems (TBMCS) used by the US Air Force (Department of the Air Force, 2010).

Doctrinally, the current method of defining area of operation is derelict in the cyber domain. Without a mapping function that allows for holistic situational awareness and targeting of cyber assets both physically and logically, the current construct for area of operation is not only incomplete and ineffectual, it also produces a stragegic blindspot that greatly increases the risk of cyber fratricide. Cyber assets should instead be mapped dynamically in the logical space using the Internet Protocol (IP) addresses associated with Media Access Control (MAC) addresses and the physical using traditional latitude and longitude. This mapping would help prevent the engagement of blue civilian assets and improve the awareness of red assets that are actually a subset of a green entity.

If the issues with the current continental staff system and its processes are not addressed, attrition of forces, assets, and capabilities due to cyber fratricide will continue to rise in the future proportionally or possibly exponentially to the increase in cyber operations. The consequences of a single incident at the fire team level could have an impact up through the combatant command level, meaning that even a linear increase in incidents could be exponentially catastrophic to operational and tactical functions.

REFERENCES:

Arquilla, J., & David Ronfeldt. (1993). “Cyberwar is coming!” Comparative Strategy 12.2: 141-165.

Department of the Air Force. (2010). “Theater Battle Management Core System – Force level and unit level.” Retrieved From https://www.fbo.gov/index?s=opportunity&mode=form&id=f348b7a7d05fafe494f079bf519c947f&tab=core&_cview=1

Joint Chiefs of Staff. (2011). Joint Publication 3-13.1: Electronic warfare. Government Printing Office, Washington DC.

Joint Chiefs of Staff. (2007a). Joint Publication 2-0: Joint intelligence. Government Printing Office, Washington DC.

Joint Chiefs of Staff. (1993). Joint Publication 3-05.5: Joint special targeting and mission planning procedures. Government Printing Office, Washington DC.

Joint Chiefs of Staff. (2007b). Joint Publication 3-60: Joint targeting. Government Printing Office, Washington DC.

Joint Chiefs of Staff. (2006). Joint Publication 5-0: Joint operation planning. Government Printing Office, Washington DC.

Mandiant. (2013). APT1: Exposing One of China's Cyber Espionage Units. Retrieved from http://www.mandiant.com/apt1

Stone, B. (2008). Pakistan Cuts Access to YouTube Worldwide. Retrieved from http://www.nytimes.com/2008/02/26/technology/26tube.html