National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

DON'T FIRE UNTIL YOU SEE THE WHITES OF THEIR 1S : PROPOSING A COMPONENT-LEVEL TARGETING CYCLE FOR CYBERSPACE OPERATIONS

Major Gary Wolfman

JCSP 44	PCEMI 44
Exercise *Solo Flight*	Exercice *Solo Flight*
Disclaimer	**Avertissement**
Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.	Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 44 – PCEMI 44
2017– 2019

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

DON'T FIRE UNTIL YOU SEE THE WHITES OF THEIR 1S: PROPOSING A COMPONENT-LEVEL TARGETING CYCLE FOR CYBERSPACE OPERATIONS

By Major Gary Wolfman

"This paper was written by a candidate attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."

« La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale. »

DON'T FIRE UNTIL YOU SEE THE WHITES OF THEIR 1S: PROPOSING A COMPONENT-LEVEL TARGETING CYCLE FOR CYBERSPACE OPERATIONS

> *To me, the most terrifying form of warfare would be if there was some simultaneous cyber attack on our grid, on the banking system, and on our transportation system. That would be quite a devastating thing, and yet in theory, absent some real protective measures, that could happen.*
>
> \- Wilbur Ross

INTRODUCTION

Among the NATO nations, Canada is unique in having designated a Joint Force Cyber Component Commander (JFCCC)[1] who is responsible for the provision of cyberspace effects in support of operations.[2] A potential reason that no other JFCCCs exist is that there are no coherent theories of military Cyber Power to tell Joint Force Commanders (JFC) what principles and frameworks apply to the Cyber Domain, or how cyber should be integrated into joint operations.

In a sense, this means that designating a JFCCC, and perhaps even declaring that there is a Cyber Domain, puts the cart before the horse. Domains of military action and the component model for Joint Force employment are modern concepts, but they were conceived of within the context of pre-existing theories of military power. Theorists, such as Mahan, Doucet and Fuller, had already published extensive theories of Naval, Air and Land Power. Practitioners, such as Guderian, had extended those theories through innovative approaches to operationalization. And, naval, air and land forces developed their own supporting planning, intelligence and targeting processes – evolved in response

[1] While there have been papers and monographs from both the US Army Command and General Staff College and the Naval War College and in journals such as Joint Force Quarterly discussing the *potential value* of a JFCCC, there are no indications that any other force has actually *established* a JFCCC.

[2] Specifically, responsible to the Designated Supported Commanders: Commander Canadian Joint Operations Command (CJOC); Commander Canadian Special Operations Forces Command (CANSOFCOM); and, Commander Canadian NORAD Region (CANR).

to the conduct of operations. There is no modern equivalent of Mahan, Doucet or Fuller theorizing about Cyber Power, let alone a Guderian or a Boyd revolutionizing Cyber Power theory.

Whether or not 'the time is right' for a Cyber Domain and a Cyber Component, Canada has them. Perennial questions about whether a Cyber Domain really ought to be considered a warfighting domain[3] have been basically rendered moot by doctrine.[4] Canada has stated its intent to conduct cyber operations in Defence Policy[5], issued a Joint Doctrine Note to provide interim doctrine and is working out how to integrate cyber operations through the targeting process.[6] Issues remain, such as the legal regimes and norms applicable to cyberspace operations[7]. But these are evolving through the conduct of operations themselves as they reveal the practice of nations. Still nascent are best practices for planning and executing cyber operations – optimizing the planning, targeting and other processes used by the Cyber Component, especially if common processes an inappropriate. In general, Operations, Plans and Intelligence already use

[3] Chris McGuffin and Paul Mitchell, "On domains: Cyber and the Practice of Warfare," *International Journal*, Volume 69(3), 2014.

[4] Canada, Department of National Defence, *Canadian Armed Forces Joint Doctrine Note 2017-02: Cyber Operations*, (Ottawa: DND, 2017), 2-2.

[5] Canada, Department of National Defence, *Strong, Secure, Engaged: Canada's Defence Policy,* (Ottawa: DND, 2017). Variations of the word cyber (cyber defence, cyber capability, etc.) appear 86 times in the document and at least five SSE initiatives relate directly to cyberspace operations – in particular Initiative 88: Develop active cyber capabilities and employ them against potential adversaries in support of government-authorized military missions.

[6] Canada, Department of National Defence, *Canadian Forces Joint Publication 3-9: Targeting,* CFJP 3-9, (Ottawa: DND, 2014); Canada, Department of National Defence, *Joint Targeting Centre of Excellence Targeting Staff Handbook*, (Ottawa: DND, 2017).

[7] Michael Schmitt, et al, *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations*, (United Kingdom: Cambridge University Press, 2017); Anna-Maria Osula and Henry Rogias (eds.), *International Cyber Norms: Legal, Policy & Industry Perspective,* (Tallinn: NATO CCD COE Publications, 2016). Note that neither of these is authoritative – as indicated, these are areas which are currently evolving – but rather each seeks to capture *the state of practice* regarding the application of law and international norms respectively.

common processes[8] but the components have their own targeting cycles, for developing component targets and for dynamically executing operations against JFC assigned targets. So, there is at least one important open question – should a Cyber Component have its own component-level targeting cycle?

This paper argues that the Cyber Component needs its own, component-level targeting cycle, and will propose one. The paper begins with a survey of domains, components and how the Joint Targeting Cycle (JTC) and component targeting cycles relate to each other. A discussion how cyber operations are unique and why that makes the JTC and existing component targeting cycles inadequate follows. Finally, a Cyber Component targeting cycle will be proposed. This will demonstrate a viable Cyber Component targeting cycle, that supports the unique characteristics of cyber operations and allows the JFCCC to meet JFC requirements and aligns targeting within the Cyber Component with the JTC.

DOMAINS, COMPONENTS AND TARGETING CYCLES

Domains

No military has a definition of the term domain,[9] although the US does define each of the traditional domains. The Maritime Domain is "the oceans, seas, bays,

[8] Operations Planning Process (OPP), Joint Intelligence Preparation of the Operational Environment (JIPOE), and so on.

[9] NATO, *Allied Joint Doctrine for Cyberspace Operations*, AJP-3.20, (NATO, 2017), 12, for one example that is also specific to cyberspace operations. NATO doctrine specifically *acknowledges* the lack of a definition and states that the Strategic Commands have simply adopted a working definition, "The sphere of interest and influence in which activities, functions, and operations are undertaken to accomplish missions and exercise control over an opponent in order to achieve desired effects." Canada actually tries to define the Cyber Domain in JDN 2017-02, but it is unfortunately circular. The JDN defines the Cyber Domain in reference to cyberspace, but then defines cyberspace as an element of the operational environment (i.e., as an element of the implied Cyber Domain).

estuaries, islands, coastal areas, and the airspace above these, including the littorals."[10] The Land Domain is "the area of the Earth's surface ending at the high water mark and overlapping with the maritime domain in the landward segment of the littorals."[11] The Air Domain is "the atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible."[12] These all align to the NATO working definition, and are consistent with each other, as these domains are geographic and each domain ends where another begins.[13]

While the US military doesn't define the Cyber Domain, it does include the idea of a domain within its definition of Cyberspace as

> A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[14]

The Cyber Domain then, is not geographic, but topological – that is to say, proximity is measured in terms of network graph traversal and not physical distance. For the traditional Maritime, Land and Air domains, the components are responsible to provide the specialist knowledge, skills and domain awareness necessary for the conduct of operations.

Components

Like domain, component is also not defined, but used implicitly in reference to concepts like the component command model for structuring Joint Task Forces. This is

[10] United States, Joint Chiefs of Staff, *DoD Dictionary of Military and Associated Terms*, (Washington DC: Joint Chiefs of Staff, 2019), 140.

[11] Ibid, 131.

[12] Ibid, 11. The Space Domain is also defined as "the area above the altitude where atmospheric effects on airborne objects become negligible," at 102. Usually the Air component is responsible for both the Air and Space domains.

[13] As in the use of *littorals* in the Maritime and Land Domains, which defines the boundary between them.

[14] United States, *DoD Dictionary*…, 57.

less of an issue because the definition of a component commander reveals the meaning of component. For example, the US defines the Joint Force Land Component Commander as

> The commander within a unified command, subordinate unified command, or joint task force responsible to the establishing commander for recommending the proper employment of assigned, attached, and/or made available for tasking land forces; planning and coordinating land operations; or accomplishing such operational missions as may be assigned.[15]

The other component commander descriptions follow the same pattern, swapping *land* for *maritime*, *air* or *special operations*. The component, then, is the "assigned, attached and/or made available for tasking…forces". This allows the construction of a parallel definition for the JFCCC[16] as the commander responsible to the Designated Supported Commander for recommending the proper employment of assigned, attached and/or made available for tasking cyber forces; planning and coordinating cyber operations; or accomplishing such operational missions as may be assigned.

Targeting Cycles

Targeting is "the process of selecting and prioritizing targets and matching the appropriate response to them, taking into account operational requirements and capabilities."[17] Targeting cycles serve two purposes: first, they provide a methodology for commanders to decide how to best achieve their objectives with the resources assigned to them; and second, they provide a methodology for commanders to ensure

[15] United States, *DoD Dictionary*…,120.

[16] Accounting for the fact that Canada doesn't commonly use US terms like subordinate unified command and prefers terms like Force Employer or Designated Supported Commander.

[17] Canada, *Canadian Forces Joint Publication 3-9: Targeting*…, 1-1

they meet their Law of Armed Conflict (LOAC) obligations while doing so.[18] This paper will not try to review the extensive body of doctrine related to targeting, but will consider how targeting at the joint and component levels interrelate.

The Joint level and the Air component share the same targeting cycles – there are two: one for deliberate planning and one for dynamic execution.[19] The relationship between them is shown at Figure 1.[20]

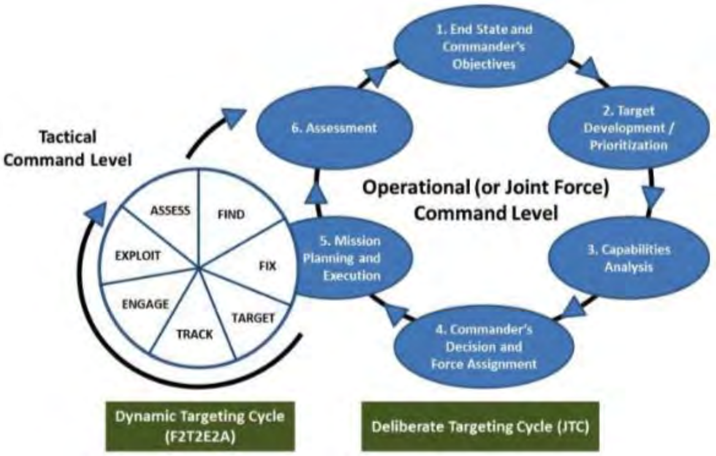
1. End State and Commander's Objectives
2. Target Development / Prioritization
3. Capabilities Analysis
4. Commander's Decision and Force Assignment
5. Mission Planning and Execution
6. Assessment
Operational (or Joint Force) Command Level
Tactical Command Level
FIND
FIX
TARGET
TRACK
ENGAGE
EXPLOIT
ASSESS
Dynamic Targeting Cycle (F2T2E2A)
Deliberate Targeting Cycle (JTC)

Figure 1 – Relationship Between the JTC and the Dynamic F2T2E2A Cycle
Source: *Canadian Forces Joint Publication 3-9 Targeting*, 4-16.

The fundamental difference is that the phases of the Air Component targeting cycle must be conducted sequentially, because they are intimately linked to the staff processes by

[18] For example, through the process of validating targets, through the use of the Collateral Damage Estimate Methodology (CDEM), and so on.

[19] There are a few things to unpack here for the interested reader. First, in the Air component targeting cycle, phases three and four of deliberate planning consist of Weaponeering and Air Tasking Order (ATO) Development, respectively. Second the JTC was developed from the Air component targeting process – e.g., capability analysis is clearly an abstraction of weaponeering. Third, the F2T2E2A dynamic cycle (some forces assume analysis without exploitation is meaningless and prefer F2T2EA) was developed in consideration of how air forces engage targets in the air, from finding them using low resolution surveillance radars to tracking them with high resolution weapon tracking systems. This is unchanged in the JTC because Joint commanders have few strike assets available to them directly (i.e., not belonging to one of the components) and those few are almost always air platforms.

[20] The figure shows the them for the Joint Targeting Cycle, not the Air component.

which the Master Air Attack Plan (MAAP) and Air Tasking Orders (ATO) are generated on a daily basis,[21] whereas the JTC phases can be conducted concurrently. Targets approved and placed on the Joint Integrated Prioritized Target List (JIPTL) and assigned to the Air component at phase four of the JTC are the primary input into the MAAP.[22]

The Land and Maritime components use the Decide-Detect-Deliver-Assess (D3A) targeting methodology.[23] When striking targets assigned to them by the JFC, the Decide function can be abbreviated, as it covers Component-level functions spanning phases one to four of the JTC. The output of the Decide phase – or phase four of the JTC – provides input for specific targeting products (as with the MAAP for the Air component). For the Land component, e.g., this would include High-Payoff Target Lists and Attack Guidance Matrices.[24]

Special Operations Forces (SOF) don't have a component-specific targeting cycle per se, using whatever cycle best suits the operation. However, the Find-Fix-Finish-Exploit-Analyze-Disseminate (F3EAD) cycle for High Value Individual (HVI) hunting is often associated with SOF because HVIs have been a focus of SOF in its counter-terrorism role.[25] F3EAD is not unique to the SOF component, [26] however, SOF are often

[21] United States, Department of the Air Force, *Air Force Doctrine Document 2-1.9*, AFDD 2-1.9, (Washington DC: Department of the Air Force, 2006), 24.
[22] Ibid, 28.
[23] United States, Department of the Army, *Army Technical Publication 3-60: Targeting*, ATP 3-60, (Washington DC: Department of the Army, 2015); United States, Department of the Navy, *Naval Tactics Techniques and Procedures 3-02.2/Marine Corps Warfare Publication 3-31.6 Supporting Arms Coordination in Amphibious Operations*, NTTP 3-02.2/MCWP 3-31.6, (Washington DC: Department of the Navy, 2004). Presumably D3A was introduced to the Navy by way of the US Marine Corps.
[24] United States, *ATP 3-60* Targeting…, 2-1 – 2-19.
[25] Charles Faint and Michael Harris, "F3EAD: Ops/Intel 'Fusion' Feeds the SOF Targeting Process," *Small Wars Journal*, last accessed 20 May 2019, https://smallwarsjournal.com/index.php/jrnl/art/f3ead-opsintel-fusion-"feeds"-the-sof-targeting-process.
[26] United States, *ATP 3-60* Targeting…, B1-B7.

best positioned to use F3EAD because of their inherent agility, specialized training and resourcing.[27] The F3EAD cycle is shown at Figure 2.

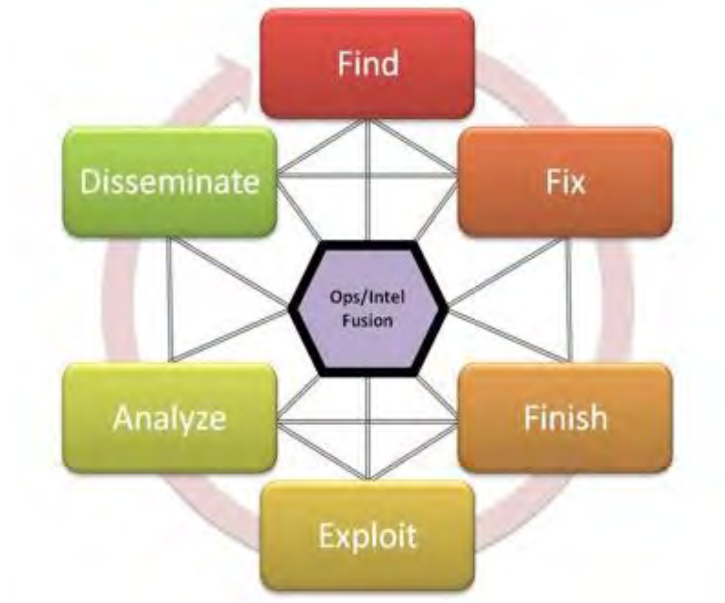

Figure 2 – The F3EAD Process
Source: Faint and Harris, "F3EAD: Ops/Intel 'Fusion' Feeds the SOF Targeting Process."

The fused Ops/Intel function will link the phases of F3EAD to the JTC and other component cycles as required – for example, to get Intelligence, Surveillance and Reconnaissance (ISR) platforms made available from the Joint level to turn a Find into a Fix, or to synchronize a Finish with a Land component Deliver and integrated fire support.

[27] Again, there are points worth unpacking for the interested reader. First, the phases are not sequential, but incorporate multiple feedback and feed forward loops, all directed by the fused Ops/Int functions. Second, the requirement for Ops/Intel fusion – which provides so much agility to the cycle is one of the key reasons that F3EAD challenges conventional forces; it doesn't fit the traditional continental staff model well. In fact, F3EAD doesn't delineate between operations and intelligence, so that conducting an operation solely to generate new intelligence is perfectly viable. Third, the analyze phase is not simply about assessing mission effectiveness (i.e., conducting BDA and making re-attack recommendations) as it is in other targeting processes. It is specifically designed to generate new Finds and Fixes.

The components use different targeting cycles because the nature of the operations they conduct in their unique domains requires them. The different targeting cycles are optimized for the nature of the domain and the component. The Cyber Component, then will likewise need its own targeting cycle if the nature of cyber operations and the characteristics of the Cyber Domain requires it.

CYBER – DIFFERENT OPERATIONS, DIFFERENT DOMAIN

Cyber Kill Chain

To understand the nature of operations in the Cyber Domain, it is useful to understand, broadly, how cyber operations work. One model is Lockheed Martin's Cyber Kill Chain, originally developed for cyber-security personnel to understand how malicious cyber actors conduct operations.[28] The Cyber Kill Chain has seven steps:

1. **Reconnaissance** - Research, identification and selection of targets
2. **Weaponization** - Coupling a remote access trojan with an exploit into a deliverable payload.
3. **Delivery** - of the weapon to the targeted environment.
4. **Exploitation** - After delivery to the victim, exploitation triggers intruders' code.
5. **Installation** - Installation of a backdoor on the victim system gives the adversary to persistence inside the target environment.
6. **Command and Control (C2)** - Once the C2 channel establishes, intruders have 'hands on the keyboard' access inside the target environment.
7. **Actions on Objectives** – Now, intruders can take actions to achieve their original objectives.[29]

Access, access, access

[28] Eric Hutchins, Michael Cloppert and Rohan Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Leading Issues in Information Warfare & Security Research*, 2011, last accessed 21 May 2019. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

[29] Ibid.

Reconnaissance and Weaponization involve the work needed to understand the target and build a capability to affect it. Cyber capabilities are extremely sensitive to the environment in which they deploy,[30] unlike munitions and other weapons with few environmental dependencies. This means simply *gaining access*[31] requires detailed knowledge of the target, and bespoke capabilities to match the target's characteristics. These first steps can take anywhere from hours to years. Delivery through Installation involves launching the attack to gain access to the system, and happens on a timescale of seconds. Only once C2 is established is the target *held at-risk*, so that actions on can be conducted. Actions on can include various forms of denial,[32] system manipulation[33] to create effects in another domain, or exfiltrating valuable intelligence. Targets could be held at-risk for months or years, as a contingency, before any action is taken.[34]

Targets within targets within targets

Gaining access to hold targets at-risk reveals the first unique aspect of the domain. Some operations will be conducted solely to gain access to a system and further develop target intelligence. And, that may not be sufficient to enable the ultimate goal, instead leading to other operations deeper within the system.

[30] United States, United States Cyberspace Command, *The USCYBERCOM Cyber Lexicon*, Version 6.3, (Fort Meade: USCYBERCOM, 2016), 17. For example, code designed to execute on a Windows operating system will generally fail to execute on a system running Linux. Code designed to exploit a particular vulnerability will fail to execute on a system where the vulnerability has been mitigated by a software update.

[31] A key issue for targeting is always whether a target the commander desires to strike can be reached. For munitions, this really comes down to the range of the strike asset protection on the target. As previously noted, however, in cyberspace range is a function of connectivity, not distance. Targets can almost always be reached in cyberspace, but there may be issues gaining access.

[32] United States, *The USCYBERCOM Cyber Lexicon*…, 23-25.

[33] Ibid, 42.

[34] The idea of holding a target at-risk is hard to reconcile with the other domains. In one sense, it is merely like having a target on a target list. Once there it is able to be selected for strike. But at-risk also implies that force is positioned to strike, which may not have a comparable, except perhaps US high-readiness nuclear forces, or US Forces Korea. At-risk may well prove to be a domain-specific concept.

Consider a hypothetical operation to hold at-risk an electrical power system. Initially, little is known about the system and there is no direct path to reach inside its network. To conduct the operation the system must be breached, and reconnaissance conducted inside the network. Suppose this reveals that the power controls are on a protected sub-network. New capabilities must be developed to bypass security and then more reconnaissance conducted inside the sub-system. And, new capabilities may again need to be developed (or existing ones modified) to finally hold the power controls at-risk.

In this example, one operation to hold a system at-risk required another operation – to breach and conduct reconnaissance – conducted recursively within it to succeed and that second operation required a third operation conducted recursively within it. This kind of recursion of operations does not occur in any of the other domains.

Our 'weapons' are different

Benitez proposed an update to the dynamic F2T2E2A cycle, to account for the evolution of the Air domain, and the speed of engagements with new autonomous and semi-autonomous weapons.[35] His arguments also apply to cyber capabilities, which have a variety of operational C2 modes.

[35] Mike Benitez, "It's About Time: The Pressing Need to Evolve the Kill Chain," *War on the Rocks*, last modified 17 May 2017, https://warontherocks.com/2017/05/its-about-time-the-pressing-need-to-evolve-the-kill-chain/. His arguments for a new targeting cycle rest on two premises: first, that the linear steps of the cycle are now distributed amongst different platforms based on their functions in a way that breaks the linear nature of the cycle. His paradigm example is the shared responsibility for the F2T2 steps within the AWACS/JSTARS/Rivet Joint 'Iron Triangle';[35] and, second, increased stand-off ranges mean that many munitions must be launched before the F2T2 steps are complete, making the issue of when engagement approval is issued challenging.

In the Lockheed Martin Cyber Kill Chain, at-risk is equated to having 'hands on keyboard' access inside a system.[36] But there are many other available C2 models for a remote access trojan, including asynchronous command via a C2 server, and autonomous or semi-autonomous operations modes.[37] In other words, depending on design, a cyber capability can act like a dumb bomb, a fire-and-forget missile, area denial mines or just about any other kind of system.

Cyber capabilities are also different from munitions in that they have unique vulnerabilities. Cyber capabilities usually need to remain covert, in order to ensure the capabilities cannot be discovered and neutralize. This is not an issue for munitions, which are expected to self-illuminate on detonation.[38] Failure to remain covert can lead to the cyber operation being discovered and sensitive capabilities falling into the hands of adversaries, and potentially co-opted by them for their own use.[39]

The casual intimacy of target development

There is a final way that cyber operations are different; they cannot be fully divorced from the JTC. The other components can accept targets from the JFC that they had no part in developing and still execute missions against them. This is not the case for the Cyber Component. If the JFC wants cyber operations options against a target, the Cyber Component must be assigned target development tasks in order to ensure that the

[36] Hutchins, Cloppert and Amin, "Intelligence-Driven Computer Network Defense" … Practitioners often refer to this as having a remote interactive shell.

[37] Asynchronous C2 allows commands to be stored on the server and the trojan to access those commands and send results back to the server for later retrieval by the operators. It allows the operation to continue even when communications are intermittent. Autonomous or semi-autonomous capabilities are pre-programmed and follow their attack parameters with no (or little) further input from an operator.

[38] It would actually be more accurate to say that for munitions this issue is never even thought about and the very idea would be considered novel.

[39] Munitions may also contain sensitive technologies, but those technologies don't survive detonation. There are already cases in the real world of cyber capabilities (e.g., Stuxnet) having been turned into cybercrime malware after having been discovered in the wild (the DuQu, Flame and Gauss families).

Cyber Kill Chain can be completed, and the target can be held at-risk, ready for final actions to be completed for the JFC. Without early tasking of the Cyber Component, there will be no access, and no time to gain access.[40]

A CYBER COMPONENT TARGETING CYCLE

Find-Fix-Finish-Feedback

A Cyber Component targeting cycle must satisfy a number of criteria. It must have a Find phase, which – as in the F3EAD cycle – includes both deliberate and opportunity-based start points and all the intelligence work to develop them.[41] The Find phase could be initiated from within the component or in response to JFC target development requirements. There must be a Fix phase to ensure there is sufficient intelligence to complete target development and execute the mission.[42] The Fix phase in particular may lead to situations where additional targeting cycles will have to be executed recursively to acquire specific target intelligence in addition to the rest of the all-source intelligence being compiled. By the end of the Fix phase, the target will be *at-risk*. During the Finish phase effects are created against the targets, either direct denial effects or manipulation effects if the end-state involves effects outside the Cyber Domain. Finally, a Feedback phase completes the cycle. Feedback involves both the generation of new intelligence derived from conducting the operation – again, as in the F3EAD cycle – and also combat assessments as in the D3A or F2T2E2A cycles.

[40] This is also sometimes referred to as the difficulty of "sprinkling magic cyber dust" onto a plan at the last minute. This problem is not unique to cyber operations but is rather common to any element for whom target development requires assets only available to the element itself. In general, this is a problem that plagues all Information-Related Capabilities.

[41] Faint and Harris, "F3EAD: Ops/Intel 'Fusion'" …

[42] Ibid.

Find-Fix-Finish-Feedback provides the main loop of the cycle, but there are other considerations which should be made explicit in the Cyber Component targeting cycle.[43] Cyber operations could be conducted recursively, begging the question of who the engagement authority for the nested operations will be.[44] Similarly if cyber capabilities can be deployed in an autonomous or semi-autonomous mode, then engagement authorities may have to issued before the capability is deployed, as there may be limited or no communications back afterwards. Conversely, in other cases, the exploitation needed to hold a target at-risk may be the most critical part of an operation (or the one most likely to be detected) and require additional oversight.

This suggests three separate authorities. First, an authority to initiate operations, including the conduct of any Reconnaissance and Weaponization activities. Second, an authority to exploit systems, in order to put them in a position where access has been gained and the target in being held at-risk. Finally, the authority to engage, which like TEA in the other domains, is the authority to strike and deliver terminal effects. The Initiation authority must be granted before starting the Find, the Exploitation authority before starting the Fix and the Engagement authority before conducting the Finish.[45] The level at which the authorities are held could vary substantially depending on the relative risk levels of Find, Fix and Finish activities, and would be expected to be issued in Strategic and Operational Targeting Directives.

[43] Target Validation and gaining Target Engagement Authority, for example, are rarely shown in the traditional targeting cycles unless they are being highlighted for very specific reasons. Instead they are treated as gateways at the beginning or end of specific phases.

[44] This is not an academic point. There is no reason to expect that the engagement authority for a denial operation against a router would have to be the engagement authority for a nested operation to exploit a firewall in order to gain access to the router.

[45] It is possible to conceive of cases where a cyberspace campaign is being executed and broad Initiation and Exploitation authorities are pre-approved against target sets.

The proposed F4 cycle is shown at Figure 3.

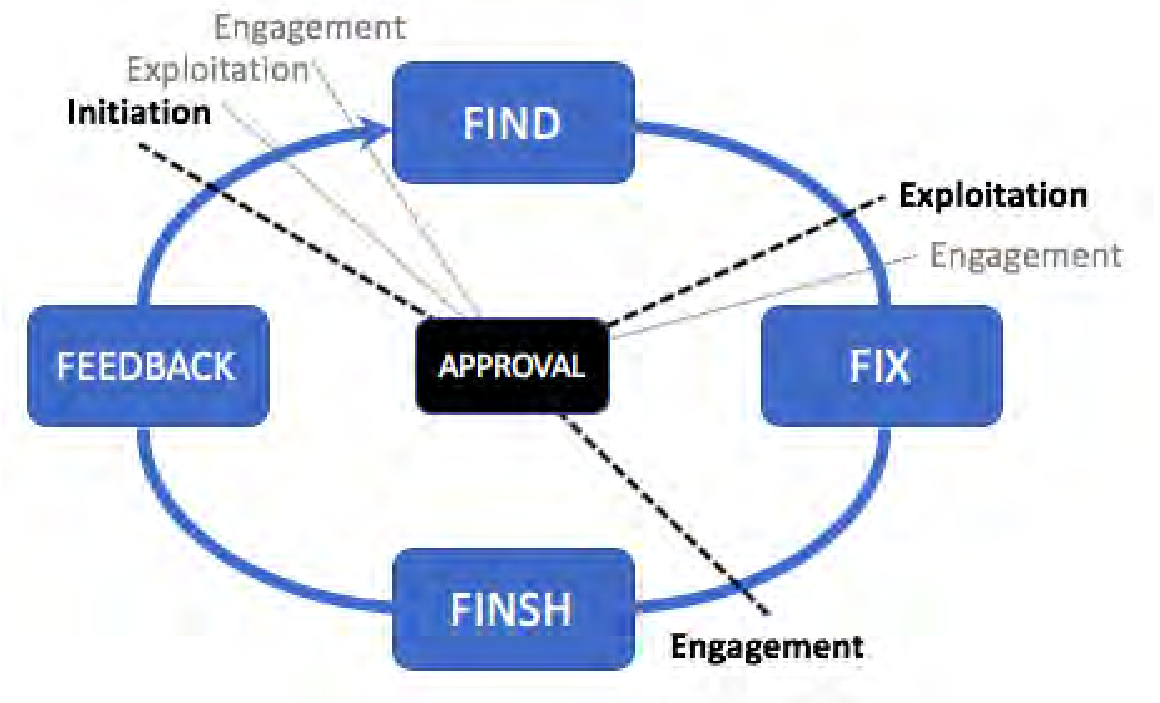

Figure 3 – F4 Cyber Component cycle
Source: Author

A Cyber Component targeting cycle works for the Cyber Domain

The F4 cycle, as shown with the required and optional authority triggers, provides the Cyber Component with a viable targeting cycle that meets its requirements for operationalizing the Cyber Domain effectively. It permits the Cyber Component to prosecute its own targets, but also provides for the necessary touchpoint to the JTC, ensuring that the Joint Force can integrate cyber into joint operations early enough to remain a viable strike option.[46] It also accounts for the unique aspects of the Cyber Domain, like the need to recursively conduct operations, that simply don't occur in the other domains.

CONCLUSION

If Canada is unique among the NATO nations in having designated Cyber as a separate component, it also has a unique opportunity to develop a Cyber Component targeting cycle. Everyone agrees that there is a unique Cyber Domain, and components operationalize domains by applying specialized processes like targeting cycles to them when appropriate. The nature of cyber operations and the Cyber Kill Chain, the need to recursively nest operations and the unique planning considerations derived from the nature of cyber capabilities (which are not shared by the other domains) all demonstrate the need for a unique targeting cycle.

The proposed Find-Fix-Finish-Feedback (F4) targeting cycle, with its associated nuanced approach to Initiation, Exploitation and Engagement authorities, provides the component-level targeting cycle that the Cyber Component requires. It accounts for the unique aspects of cyber operations and the Cyber Domain, the unique nature of cyber capabilities and provides the Cyber Component with a targeting framework to use for applying their specialist knowledge in support of the JFC's requirements. Finally, it provides a start point for the JFC to use in conceiving how cyber operations should be integrated into joint operations.

[46] This also means that the Cyber Component target cycles implicitly has the necessary touchpoints into the other component targeting cycles to permit supporting operations to be conducted by either side.

BIBLIOGRAPHY

Benitez, Mike. “It’s About Time: The Pressing Need to Evolve the Kill Chain.” *War on the Rocks*. Last modified 17 May 2017. https://warontherocks.com/2017/05/its-about-time-the-pressing-need-to-evolve-the-kill-chain/.

Canada. Department of National Defence. *Canadian Armed Forces Joint Doctrine Note 2017-02: Cyber Operations*. Ottawa: DND, 2017.

Canada. Department of National Defence. *Canadian Forces Joint Publication 3-9: Targeting*. CFJP 3-9. Ottawa: DND, 2014.

Canada. Department of National Defence. *Joint Targeting Centre of Excellence Targeting Staff Handbook*. Ottawa: DND, 2017.

Canada. Department of National Defence. *Strong, Secure, Engaged: Canada’s Defence Policy*. Ottawa: DND, 2017.

Faint, Charles and Michael Harris. “F3EAD: Ops/Intel ‘Fusion’ Feeds the SOF Targeting Process.” *Small Wars Journal*. Last accessed 20 May 2019. https://smallwarsjournal.com/index.php/jrnl/art/f3ead-opsintel-fusion-“feeds”-the-sof-targeting-process.

France. Commandement de la cyberdéfense. *Éléments publiques de doctrine militaire de lutte informatique offensive*. Paris : Ministère des armées, 2019.

Hutchins, Eric, Michael Cloppert and Rohan Amin. “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.” *Leading Issues in Information Warfare & Security Research*. 2011. Last accessed 21 May 2019. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

McGuffin, Chris and Paul Mitchell. “On domains: Cyber and the Practice of Warfare.” *International Journal*, Volume 69(3), 2014.

NATO. *Allied Joint Doctrine for Cyberspace Operations*. AJP-3.20. NATO, 2017.

Osula, Anna-Maria and Henry Rogias (eds.). International Cyber Norms: Legal, Policy & Industry Perspectives. Tallinn: NATO CCD COE Publications, 2016.

Schmitt, Michael, et al. *Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations*. United Kingdom: Cambridge University Press, 2017.

Schmitt, Michael. “The Law of Cyber Targeting.” *Naval War College Review*, Volume 68, Issue 2, 2015.

Smart, Steven. “Joint Targeting in Cyberspace.” *Air & Space Power Journal*, Volume 25, Issue 4 (Winter 2011), 2011: 65-75.

United States. Department of the Air Force. *Air Force Doctrine Document 2-1.9*. AFDD 2-1.9. Washington DC: Department of the Air Force, 2006.

United States. Department of the Army. *Army Technical Publication 3-60: Targeting*. ATP 3-60. Washington DC: Department of the Army, 2015.

United States. Department of the Navy. *Naval Tactics Techniques and Procedures 3-02.2/Marine Corps Warfare Publication 3-31.6 Supporting Arms Coordination in Amphibious Operations*. NTTP 3-02.2/MCWP 3-31.6. Washington DC: Department of the Navy, 2004.

United States. Joint Chiefs of Staff. *Combined Joint Chiefs of Staff Instruction 3370.01B: Target Development Standards*. Washington DC: Joint Chiefs of Staff, 2016.

United States. Joint Chiefs of Staff. *DoD Dictionary of Military and Associated Terms*. Washington DC: Joint Chiefs of Staff, 2019.

United States. Joint Chiefs of Staff. *Joint Publication 3-12: Cyberspace Operations*. JP 3-12. Washington DC: Joint Chiefs of Staff, 2018.

United States. Joint Chiefs of Staff. *Joint Publication 3-60: Targeting*. JP 3-60. Washington DC: Joint Chiefs of Staff, 2018.

United States. United States Cyberspace Command. *The USCYBERCOM Cyber Lexicon*. Version 6.3. Fort Meade: USCYBERCOM, 2016.