The Unified Kill Chain

RAISING RESILIENCE AGAINST ADVANCED CYBER ATTACKS

#	Attack Phase	Description
1	**Reconnaissance**	*Researching, identifying and selecting targets using active or passive reconnaissance.*
2	**Weaponization**	*Preparatory activities aimed at setting up the infrastructure required for the attack.*
3	**Delivery**	*Techniques resulting in the transmission of a weaponized object to the targeted environment.*
4	**Social Engineering**	*Techniques aimed at the manipulation of people to perform unsafe actions.*
5	**Exploitation**	*Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.*
6	**Persistence**	*Any access, action or change to a system that gives an attacker persistent presence on the system.*
7	**Defense Evasion**	*Techniques an attacker may specifically use for evading detection or avoiding other defenses.*
8	**Command & Control**	*Techniques that allow attackers to communicate with controlled systems within a target network.*
9	**Pivoting**	*Tunneling traffic through a controlled system to other systems that are not directly accessible.*
10	**Discovery**	*Techniques that allow an attacker to gain knowledge about a system and its network environment.*
11	**Privilege Escalation**	*The result of techniques that provide an attacker with higher permissions on a system or network.*
12	**Execution**	*Techniques that result in execution of attacker-controlled code on a local or remote system.*
13	**Credential Access**	*Techniques resulting in the access of, or control over, system, service or domain credentials.*
14	**Lateral Movement**	*Techniques that enable an adversary to horizontally access and control other remote systems.*
15	**Collection**	*Techniques used to identify and gather data from a target network prior to exfiltration.*
16	**Exfiltration**	*Techniques that result or aid in an attacker removing data from a target network.*
17	**Impact**	*Techniques aimed at manipulating, interrupting or destroying the target system or data.*
18	**Objectives**	*Socio-technical objectives of an attack that are intended to achieve a strategic goal.*

Author:

Paul Pols

Special thanks to:

Francisco Dominguez

Fox-IT

Executive Summary

Organizations increasingly rely on Information and Communication Technology (ICT). This reliance exposes them to growing risks from cyber attacks from a range of threat actors. The term Advanced Persistent Threats (APTs) is used to refer to particularly capable and persistent threat actors. In this white paper, a Unified Kill Chain (UKC) model is presented that details the tactics that form the building blocks of cyber attacks by APTs. The Unified Kill Chain provides insights into the ordered arrangement of phases in attacks from their beginning to their completion, by uniting and extending existing models. The Unified Kill Chain can be used to analyze, compare and defend against targeted and non-targeted cyber attacks.

Research shows that the traditional Cyber Kill Chain® (CKC), as presented by researchers of Lockheed Martin, is perimeter- and malware-focused. As such, the traditional model fails to cover other attack vectors and attacks that occur behind the organizational perimeter. The Unified Kill Chain offers significant improvements over these scope limitations of the CKC and the time-agnostic nature of the tactics in MITRE's ATT&CK™ model (ATT&CK). Other improvements over these models include: explicating the role of users by modeling *social engineering*, recognizing the crucial role of choke points in attacks by modeling *pivoting*, covering the compromise of *integrity* and *availability* in addition to confidentiality and elucidating the overarching *objectives* of threat actors.

#	*Unified Kill Chain*
1	***Reconnaissance***
2	***Weaponization***
3	***Delivery***
4	***Social Engineering***
5	***Exploitation***
6	***Persistence***
7	***Defense Evasion***
8	***Command & Control***
9	***Pivoting***
10	***Discovery***
11	***Privilege Escalation***
12	***Execution***
13	***Credential Access***
14	***Lateral Movement***
15	***Collection***
16	***Exfiltration***
17	***Impact***
18	***Objectives***

The case studies that were performed also falsify a crucial assumption underlying traditional kill chain models, namely that attackers must progress successfully through each phase of a deterministic sequence. The observation that attack phases may be bypassed affects defensive strategies fundamentally, as an attacker may also bypass the security controls that apply to these phases. Instead of focusing on thwarting attacks at the earliest point in time, layered defense strategies that focus on attack phases that occur with a higher frequency or that are vital for the formation of an attack path are thus expected to be more successful. These insights support the development (or realignment) of layered defense strategies that adopt the *assume breach* and *defense in depth* principles and to optimize the return on investment (ROI) of their security measures.

As the reliance of organizations on ICT continues to grow, and APT attacks continue to rise in number and in force, the risks for organizations and societies as a whole increase at an accelerating pace. The Unified Kill Chain attack model can be used in the areas of prevention, detection, response and intelligence to develop and realign defense strategies in an attempt to raise the resilience of organizations and societies against this dangerous trend.

Keywords — Unified Kill Chain, Cyber Security, Strategy, Attack Modeling, Attack Simulation, Threat Emulation, Cyber Kill Chain®, MITRE ATT&CK™, Red Team, Tactics, Techniques, Procedures, Assume Breach, Defense in Depth.

Table of Contents

1 Introduction

In the last decades, the dependence throughout modern societies on information and communication technology (ICT) has continued to rise. Vulnerabilities in the supporting ICT assets increasingly threaten critical activities that depend on ICT within organizations and society as a whole. Organizations need to protect their critical assets against a variety of threat actors that range from cyber criminals to nation states.

To properly defend oneself against advanced cyber attacks, one must first understand how these attacks are typically performed. For this purpose, threat modeling is required [1]. The Cyber Kill Chain® by Lockheed Martin (CKC) was traditionally regarded as the industry standard threat model for defending against advanced cyber attacks [2]. Despite (or because of) its prominent status, the CKC has been widely criticized. The most damaging criticisms argue that the CKC is perimeter- and malware-focused [3]. A more comprehensive model is required to deal with advanced cyber attacks beyond the organizational perimeter and beyond malware attacks.

The term “kill chain” describes an *end-to-end* process [2], or the entire chain of events, that is required to perform a successful attack. Once an attack is understood and deconstructed into discrete phases, it allows defenders to map potential countermeasures against each one of these phases. Kill chain and other attack lifecycle models, can thus help defenders understand and defend against the increasingly complex attacks that they are facing. Advanced cyber attacks typically extend beyond exploiting one vulnerability in an internet-connected system. Depending on the security posture of the target, attacks may require attackers to forge an attack path through the internal network of the victim, in which multiple correlated vulnerabilities are exploited before critical assets can be targeted and objectives can be achieved.

The aim of this white paper is to present the *Unified Kill Chain*, that can serve to model and defend against cyber attacks, from the attacker’s first steps to the achievement of an adversarial objective. The model was designed to defend against end-to-end cyber attacks from a variety of advanced attackers, including so-termed Advanced Persistent Threats (APTs) [4]. These types of actors may range from financially motivated enterprise ransomware groups to the espionage and sabotage campaigns by nation states. The model has also successfully been applied to defend against ransomware worms, that implement tactics that were previously primarily seen in targeted attacks. As such, the Unified Kill Chain has a proven track recording in raising the resilience of targeted organizations against a range of targeted and (initially) untargeted attacks.

The Unified Kill Chain offers a substantiated basis for strategically realigning defensive capabilities and cyber security investments within organizations, in the areas of prevention, detection, response and intelligence. The Unified Kill Chain allows for a structured analysis and comparison of threat intelligence regarding the tactical modus operandi of attackers. In the area of prevention, the Unified Kill Chain can be used to map countermeasures to the discrete phases of an attack. Detection can be prioritized based on the insights into the ordered arrangement of the attack phases. In emergency response situations, the Unified Kill Chain aids investigators in triage and modeling likely attacks paths. The model also specifically allows for the improvement of the predictive value of Red Team threat emulations, which aim to test the security posture of organizations in these areas.

2 Design of the Unified Kill Chain

The Unified Kill Chain was developed through a hybrid research approach, combining design science with qualitative research methods. The model was first published in the Executive Master's thesis of Paul Pols entitled "*The Unified Kill Chain: modeling Fancy Bear attacks*" at the Cyber Security Academy[1]. The Unified Kill Chain extends and combines existing models, such as Lockheed Martins' Cyber Kill Chain® [2] and MITRE's ATT&CK™ for Enterprise[5]. This white paper offers a concise overview of the Unified Kill Chain model and its development, as depicted in Table 1.

Table 1 - Overview of the development of the Unified Kill Chain

#	Unified Kill Chain	Cyber Kill Chain® [2]	Lalliberte [6]	Nachreiner [7]	Bryant [8]	Malone [9]	MITRE ATT&CK™ [5]	UKC after literature study	UKC after RT case study 1	UKC after RT case study 2	UKC after RT case study 3	UKC after RT case studies	The Unified Kill Chain
1	*Reconnaissance*	1	1	1	1	1		1	1	1	1	1	1
2	*Weaponization*	2	3	3	3	2		2	2	2	2	2	2
3	*Delivery*	3	5	5	6	3		7	7	3	3	3	3
4	*Social Engineering*	5	6	6	11	5		3	3	4	4	4	4
5	*Exploitation*	6	8	8	14	6		5	4	5	5	5	5
6	*Persistence*	8	14	9	18	8	6	6	5	6	6	6	6
7	*Defense Evasion*	18	18	14	16	10	11	8	6	7	7	7	7
8	*Command & Control*			18		5	7	9	8	8	8	8	8
9	*Pivoting*					11	13	11	9	9	9	9	9
10	*Discovery*					14	10	10	11	11	11	10	10
11	*Privilege Escalation*					17	14	14	10	10	10	11	11
12	*Execution*					18	12	12	14	14	14	12	12
13	*Credential Access*						15	13	12	12	12	13	13
14	*Lateral Movement*						16	17	13	13	13	14	14
15	*Collection*						8	15	17	17	17	17	15
16	*Exfiltration*							16	15	15	15	15	16
17	*Impact*								16	16	16	16	17
18	*Objectives*												18

In the hybrid research approach, the strengths and weaknesses of traditional kill chain models were studied through literature review (the spectrum between white and black in the first row of table 1). Potential amendments to remedy tactical shortcomings were identified and a first hypothesis for a unified kill chain was designed. The first hypothesis for a unified kill chain was iteratively evaluated and improved through real world case studies (the green spectrum in the first row of table 1). Firstly, three case studies were performed into the transparent cyber attacks by Fox-IT's Red Team (RT). Finally, the model was evaluated and refined by modeling the attacks of APT28 alias Fancy Bear. The (intermediate) results were validated through semi-structured interviews. The results of the research culminated in the Unified Kill Chain [1].

3 Phases of the Unified Kill Chain

3.1 Overview of the attack phases

Modern cyber attacks are typically phased progressions towards strategic objectives. Cyber attacks and threat actors can be described using Tactics, Techniques and Procedures (TTPs). The Unified Kill Chain describes attacks on the tactical level, at which activities are directed to achieve the objectives of an attack [10]. When the ordered arrangement (or sequence) in which tactics occur is considered, tactics can be regarded as the phases of an attack. The tactical representation of actions as attack phases can remain similar across multiple attacks, even if specific Techniques and Procedures are changed on the operational level [11].

Through the previously described hybrid research approach, 18 tactics were identified that can be used to describe the phases of modern cyber attacks[1]. The following table defines the individual attack phases and provides insight into their expected ordered arrangement.

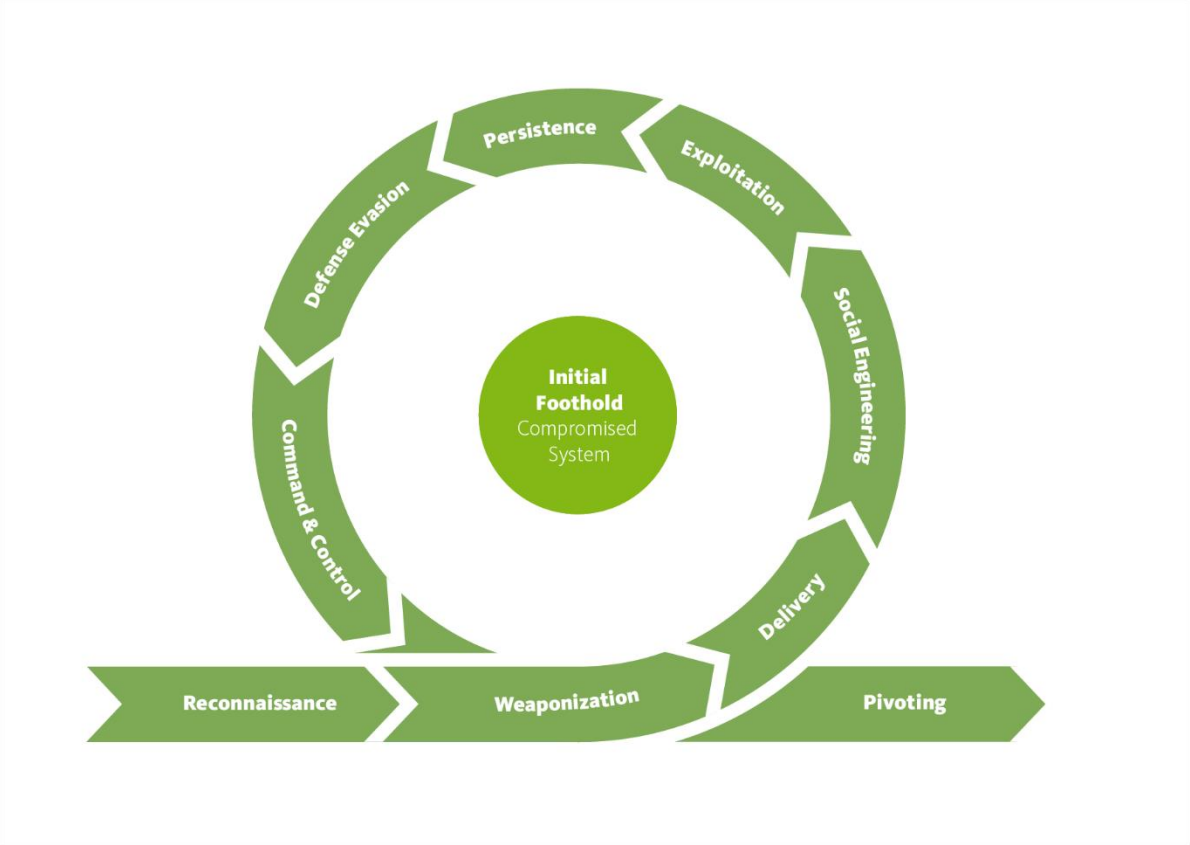
The Unified Kill Chain		
1	***Reconnaissance***	*Researching, identifying and selecting targets using active or passive reconnaissance.*
2	***Weaponization***	*Preparatory activities aimed at setting up the infrastructure required for the attack.*
3	***Delivery***	*Techniques resulting in the transmission of a weaponized object to the targeted environment.*
4	***Social Engineering***	*Techniques aimed at the manipulation of people to perform unsafe actions.*
5	***Exploitation***	*Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.*
6	***Persistence***	*Any access, action or change to a system that gives an attacker persistent presence on the system.*
7	***Defense Evasion***	*Techniques an attacker may specifically use for evading detection or avoiding other defenses.*
8	***Command & Control***	*Techniques that allow attackers to communicate with controlled systems within a target network.*
9	***Pivoting***	*Tunneling traffic through a controlled system to other systems that are not directly accessible.*
10	***Discovery***	*Techniques that allow an attacker to gain knowledge about a system and its network environment.*
11	***Privilege Escalation***	*The result of techniques that provide an attacker with higher permissions on a system or network.*
12	***Execution***	*Techniques that result in execution of attacker-controlled code on a local or remote system.*
13	***Credential Access***	*Techniques resulting in the access of, or control over, system, service or domain credentials.*
14	***Lateral Movement***	*Techniques that enable an adversary to horizontally access and control other remote systems.*
15	***Collection***	*Techniques used to identify and gather data from a target network prior to exfiltration.*
16	***Exfiltration***	*Techniques that result or aid in an attacker removing data from a target network.*
17	***Impact***	*Techniques aimed at manipulating, interrupting or destroying the target system or data.*
18	***Objectives***	*Socio-technical objectives of an attack that are intended to achieve a strategic goal.*

Multiple tactical phases of an attack can be combined to achieve intermediate goals, such as gaining an initial foothold in a targeted network, propagating through the network to expand the level of access and performing actions on critical assets. The next sections will describe how the individual phases of the Unified Kill Chain are typically combined by attackers to achieve intermediate goals in the phased progression towards achieving their final objectives.

[1] When phases are used as building blocks to model attacks, it is recommended to use the most specific description of an activity to focus on what an attacker aims to accomplish tactically. For example, the *Exploitation* of a vulnerability can be used for the *Execution* of code solely to obtain *Privilege Escalation*, which can collectively occur within a split second in a way that is transparent for the attacker. These entwined activities can thus all be described as *Privilege Escalation*, to simplify the resulting kill chain.

3.2 Initial foothold

The objectives of an attack may require an attacker to gain access to systems or data that are only accessible within a trusted environment, typically within the internal network of a targeted organization. To gain access to these systems or data, an attacker can employ the first phases of the Unified Kill Chain to breach the organizational perimeter and gain an initial foothold in the network.

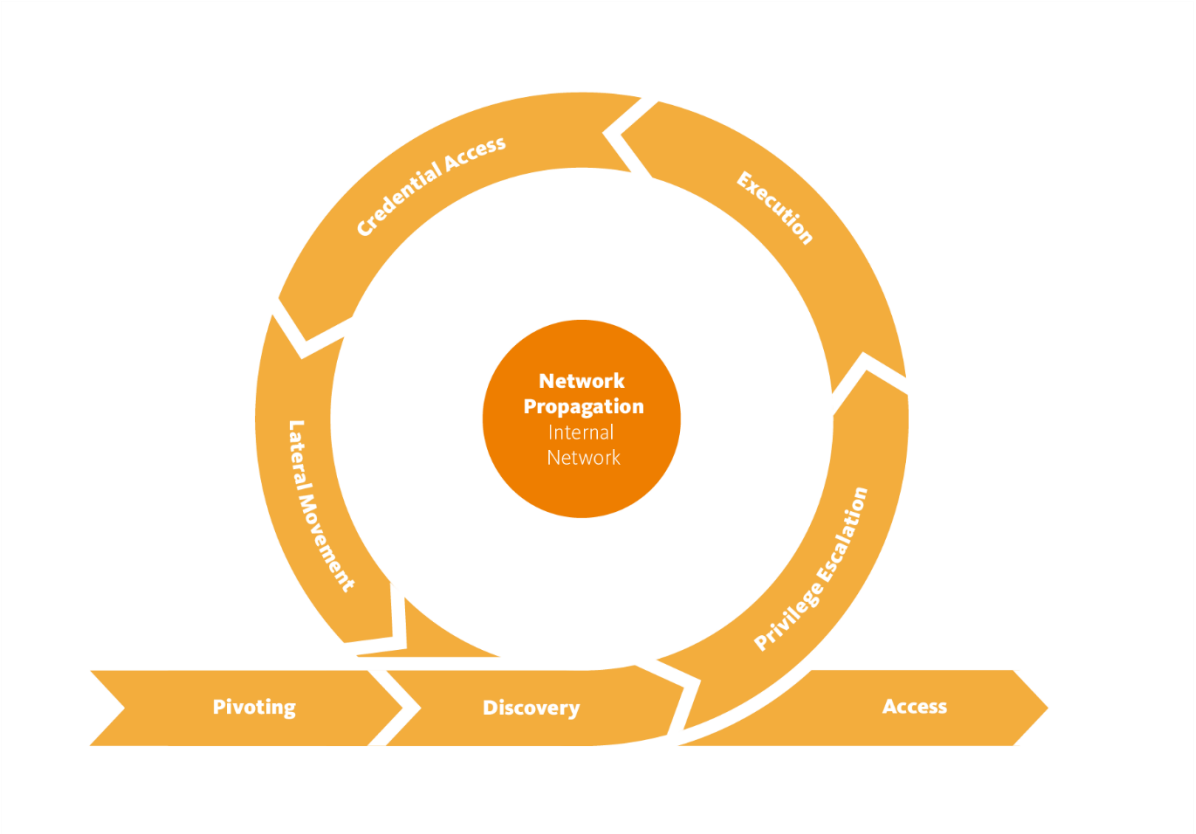


Cyber attacks are typically initiated from the external perspective of an anonymous attacker on the internet. To enhance the chance of success, a target may be researched first (*Reconnaissance*). Further preparatory activities may include setting up an attack infrastructure, which can include weaponizing objects and command & control servers (*Weaponization*). The weaponized object can be delivered to the target through a variety of means, such as (spear) phishing, watering hole or supply chain attacks (*Delivery*). The weaponized object may be triggered by manipulating a user to perform unsafe actions (*Social Engineering*) or by exploiting a vulnerability (*Exploitation*). Once executed, the weaponized object may be used to acquire persistent access to the system (*Persistence*). Specific actions may be taken in an attempt to remain undetected (*Defense Evasion*). Lastly, a compromised system generally establishes a communication channel with an attacker-controlled system on the internet (*Command & Control*).

If one of these tactics fail, the attempt to gain an initial foothold in a targeted network may also fail. However, an attacker may change tactics, or adjust the specific techniques used within a tactic, in follow-up attacks until the strategic goal of gaining an initial foothold is achieved. The first part of the phased progression of an attacker in a cyber attack, namely to gain an initial foothold in a target network, may thus be regarded as a loop. If access to the compromised system directly allows an attacker to take action on the final objectives of the attack, then an attacker can move straight to Action on Objectives. If the objectives require further access to systems and data, an attacker will be forced to propagate through the internal network first.

3.3 Network propagation

Once an attacker has acquired access to a targeted network, additional privileges may be required to gain access to assets that allow the attacker to perform actions on the objectives of the attack. Network propagation refers to the activities that attackers typically perform to gain additional access to systems and data in furtherance of their objectives. These activities may be performed by an external attacker that has acquired digital or physical access behind the organizational perimeter, typically by compromising one system, through attack vectors such as (spear) phishing, a watering hole attack, a supply chain attack or through an insider threat.



If the perimeter of an organization was breached by compromising a system, an attacker may first focus on that system. This can consist of gathering information about the compromised system, such as enumerating the privileges of users and accessible data (a local form of *Discovery*). If the attacker has restricted privileges on the compromised system, privileges may be escalated vertically to a higher level, typically by exploiting a vulnerability or a misconfiguration (a local form of *Privilege Escalation*). The escalated privileges can allow an attacker to execute arbitrary code on the system with elevated privileges (*Execution*). The ability to execute code can amongst others be used to acquire credentials from the local system, through the extraction of credentials from the hard disk or from memory (*Credential Access*).

Alternatively, an attacker may merely use the initially compromised system as a pivot point to attack other systems in the network (*Pivoting*). A variety of techniques can be used that are aimed at identifying potential vulnerabilities in other systems (a remote form of *Discovery*). Vulnerabilities that are identified in other systems on the network may be exploited for the vertical escalation of privileges (a remote form of *Privilege Escalation*). The acquired privileges may allow for remote code execution on the system (*Execution*), which may then be leveraged to extract credentials from the hard disk or from memory of the remote system (*Credential Access*).

Once credentials have been acquired that can provide control over other systems, an attacker may horizontally escalate privileges to these systems (*Lateral Movement*). Control over these systems may allow for the extraction of additional credentials (*Credential Access*). This process can be performed iteratively, until access to the targeted assets is eventually acquired. In networks where network segmentation and identity access management (IAM) isolation have been strictly applied, an attacker will have to go through this process for every segment in the path towards the critical assets. Consequently, the process of propagating through a targeted network towards critical assets can be regarded as a loop until the required access to critical assets is obtained.

3.4 Action on Objectives

By gaining an initial foothold in a targeted network, and propagating through the network as required, an attacker can acquire the privileges that are necessary to eventually perform actions on the objectives of the attack.

When the objective of an attack involves compromising the availability or integrity of an asset, it may suffice to use the acquired privileges to manipulate, interrupt or destroy the target (*Impact*)[2]. If the objective involves compromising the confidentiality of an asset, additional techniques may be employed to collect the data that the attacker is after (*Collection*). Collected data may be exfiltrated to an attacker-controlled system (*Exfiltration*), until the objectives are achieved.

[2] When the Unified Kill Chain was first developed, MITRE's ATT&CK™ framework did not include a tactic that covered attacks on the availability and integrity of systems or data. The Unified Kill Chain introduced an attack phase to cover these activities under the name *Target Manipulation*. Since the Unified Kill Chain was first published in December of 2017, MITRE has introduced the *Impact* tactic in v4.0 of its model in April of 2019, that covers the same activities. To maintain a uniform language between these attack models, the Target Manipulation phase in the Unified Kill Chain has been renamed to Impact.

Collectively the phases Collection, Exfiltration and Impact can be used to describe all compromises of the Confidentiality, Integrity and Availability (CIA) triad. The term Action on Objectives can be used to refer to these collective objective-specific phases on a more abstract level. These activities can be performed continuously or periodically and can thus also be regarded as a loop.

The Unified Kill Chain also explicitly includes the socio-technical objectives of an attacker (*Objectives*). Explicitly defining the adversarial objectives is expected to be beneficial for gaining a deeper level of understanding of the attacker activities. For example, when the objectives of an attacker are known, it may be possible to predict which assets are more likely to be targeted in furtherance of those objectives. This in turn will help to predict and defend the attack paths towards those assets. While it may not be easy to counteract the objectives phase specifically, relevant measures can be prepared to help deal with a successful compromise. For example, a proactive incident management communication strategy can be adopted to pre-empt the release of (mis)information following a compromise.

4 Using the Unified Kill Chain

4.1 Modeling specific cyber attacks and threat actors

The Unified Kill Chain offers insights into the tactics that attackers employ in advanced cyber attacks and the order in which they typically, but not necessarily, occur. The phases that are part of the Unified Kill Chain can also be used as building blocks to describe the behavior of attackers in individual cyber attacks (an *attack specific* kill chain), or to describe the tactical modus operandi of an attacker (an *actor specific* kill chain), by putting them in the right order as observed in a specific attack or in the typical modus operandi of an attacker.

The *attack specific* kill chains can be used to analyze the intricacies of individual attacks. Multiple attack specific kill chains can be compared to show how these attacks converge or diverge on a tactical level and to realign defenses accordingly. The *actor specific* kill chains demonstrate the tactics that are in a specific actor's repertoire in their presumable ordered arrangement. As such, an actor specific kill chain encompasses all tactics that have been observed in the attacks by that threat actor and forms the relevant subset of the UKC for that threat actor. In defending against the threat actor, a defense strategy can be created with the relevant tactics (as potential attack phases) in mind.

The length of a kill chain that describes an individual attack depends on the amount of different tactics that an attacker needs to use to reach their objective. As such, the length of the attack specific kill chains is determined in large part by the combination of the modus operandi of an attacker and the defensive posture of targeted organizations. The stronger the security posture, the longer the kill chain is expected to be.

4.2 Realigning defensive strategies

The research that was performed by Paul Pols into advanced cyber attacks [1] falsifies a crucial assumption underlying Lockheed Martin's Cyber Kill Chain® (CKC), namely that an attacker "*must progress successfully through each stage of the chain before it can achieve its desired objective; just one mitigation disrupts the chain and the adversary*" [2, p. 2]. In individual attacks, some tactics may occur out of their expected sequence or be bypassed altogether. The research challenges the foundational assumption that attacks can by thwarted by disrupting any one of the phases in the chain of events. Based on this original assumption, defenders may naturally focus their efforts on disrupting cyber attacks at the earliest phases of an attack.

The fact that attack phases may be bypassed affects defensive strategies fundamentally. In bypassing an attack phase, an attacker may also bypass the security controls that apply specifically to that phase. Instead of focusing on thwarting attacks at the earliest point in time, defensive strategies that focus on phases that either occur with a higher frequently or that are vital for the formation of an attack path towards an asset are expected to be more successful. This notably includes creating, securing and monitoring choke points that force attackers to pivot and start anew before they can act on their objectives. These choke points can be created through measures such as network segmentation in combination with the isolation of identity and access management zones.

It is challenging to prevent the compromise of every single internet connected system in a large network, while the number of critical supporting assets is typically far more limited. Strategies that aim to defend a limited amount of critical supporting assets may thus be more likely to succeed than strategies that aim to defend all internet connected systems. Furthermore, the objectives of an attacker may force them to find an attack path within the confines of the internal network of the targeted organization, which takes place within the locus of control of defenders. Organizations can therefore potentially significantly increase their resilience, by focusing their efforts on the attack phases that occur within the confines of their internal network that pave the way to act on the objectives.

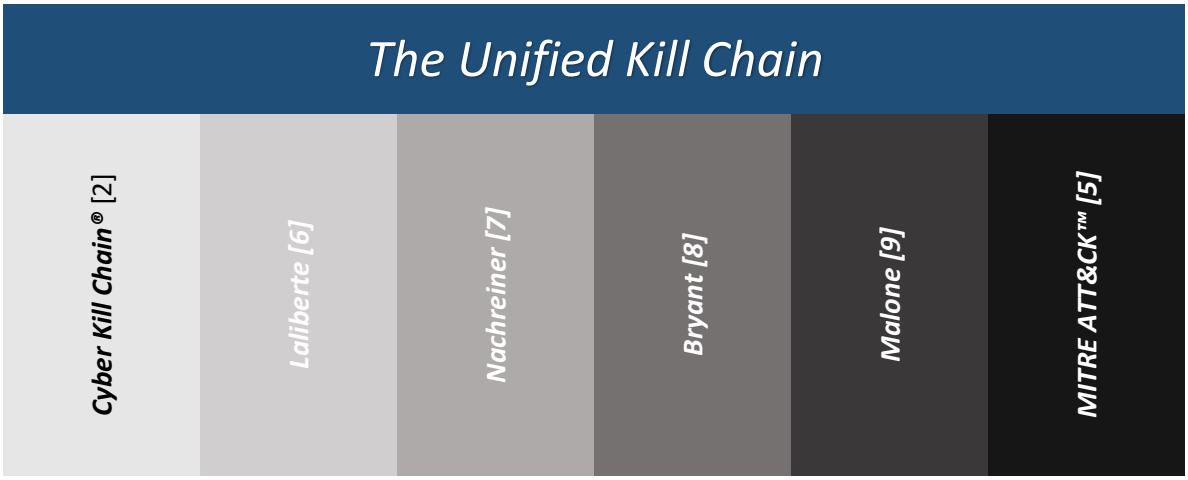
4.3 Scope of the Unified Kill Chain

The Unified Kill Chain can be used to model all activities that typically occur during cyber attacks, from the very first exploratory activities of external attackers until the final objectives of an attack are achieved behind the organizational perimeter. To cover this broad scope, the Unified Kill Chain stands on the shoulders of giants, including but not limited to Lockheed Martins' Cyber Kill Chain® [2] and MITRE's ATT&CK™ for Enterprise model [5]. The incorporation of relevant phases (Cyber Kill Chain®) and tactics (ATT&CK™) into a unified model, allows cyber security professionals to seamlessly combine and extend the collective explanatory power to model modern cyber attacks.

	Cyber Kill Chain®	MITRE ATT&CK™	Unified Kill Chain
Reconnaissance	√	✖	√
Weaponization	√	✖	√
Delivery	√	√	√
Social Engineering	✖	✖	√
Exploitation	√	✖	√
Persistence	√	√	√
Defense Evasion	✖	√	√
Command & Control	√	√	√
Pivoting	✖	✖	√
Discovery	✖	√	√
Privilege Escalation	✖	√	√
Execution	✖	√	√
Credential Access	✖	√	√
Lateral Movement	✖	√	√
Collection	✖	√	√
Exfiltration	✖	√	√
Impact	✖	√	√
Objectives	√	✖	√

4.4 Additional improvements in the Unified Kill Chain

The Unified Kill Chain is the product of a hybrid scientific research approach, which integrated a multitude of otherwise conflicting views on kill chain and attack lifecycle models (as depicted in the table below).

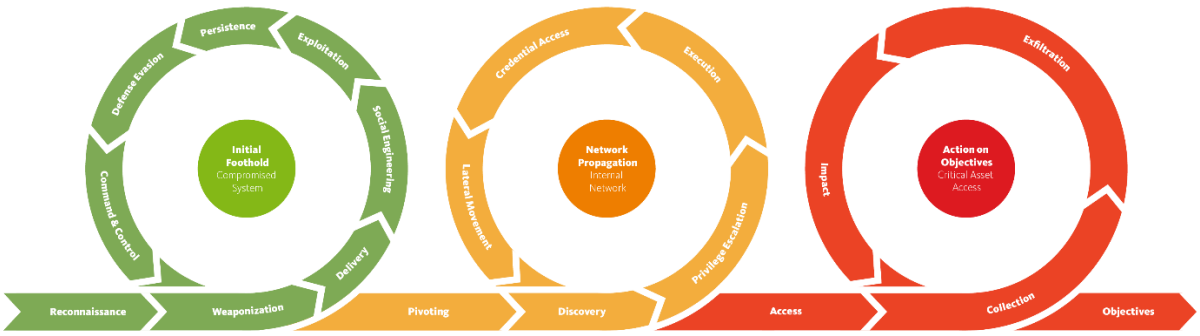


The Unified Kill Chain provides several improvements over these pre-existing models. The following improvements are particularly noteworthy:

- By contextualizing the time-agnostic tactics of ATT&CK™ within a kill chain model, the Unified Kill Chain provides insights into the ordered arrangement of these tactics, thus showing the order within which the tactics typically occur as phases in actual attacks. The Unified Kill Chain also explains why tactics occur in sets of distinct sequences as phases within attacks, which is valuable in developing an adequate defense-in-depth strategy.
- A broader interpretation of the *Weaponization* phase overcomes previous criticisms on the presence of this phase in kill chain models. The redefined Weaponization phase makes logically distinct, relevant and observable preparatory attacker activities actionable. In the case studies, this could have led to the early detection of imminent attacks, for example when typo-squatted phishing domains were registered in setting up an attack infrastructure.
- The Unified Kill Chain explicitly separates *Social Engineering* from *Exploitation*, thereby making the role that users play in the execution of attacks explicit. Too often users are regarded as the weakest link in the chain, while they should be regarded as the first line of defense. If users are knowledgeable about their role in securing the critical assets and learn appropriate behaviors, they can function as an early warning system for attempts to gain an initial foothold. Furthermore, when mapping countermeasures against the attack phases, the distinction between Social Engineering and Exploitation is required to ensure that a variety of relevant countermeasures are implemented.
- The Unified Kill Chain is suitable for a broad range of potential attacker objectives, such as sabotage and manipulation in addition to the traditional focus on espionage. To do so, the Unified Kill Chain covers the Confidentiality, Integrity and Availability (CIA) cyber security triad in full, by modeling *Impact* (formerly known as Target Manipulation) in addition to Collection and Exfiltration. The Unified Kill Chain also makes the *Objectives* of attackers explicit, which encourages defenders to take the strategic objectives of attackers into account, which is expected to be beneficial for a deeper level of understanding of the interconnection of attacker activities as well as to focus on the assets which attackers are likely to target.

5 Conclusion

The primary driver for white paper was to raise the resilience of organizations and societies against cyber attacks by improving attack modeling. Without a thorough understanding of how modern attacks take place, investments in defensive capabilities are expected to be inefficiently distributed over the attack surface of organizations. The Unified Kill Chain is therefore intended to provide insight into the attack phases that advanced attackers typically go through when performing modern cyber attacks.



A conventional belief within cyber security is that attackers have the upper hand, because they only need to exploit one defensive flaw (the defeatist adage). Lockheed Martin's Cyber Kill Chain® promised a fundamentally reversed balance, by claiming that defenders could prevail by disrupting attackers at any point in their deterministically phased progression. The balance between attackers and defenders that is suggested by the Unified Kill Chain is much more delicate. Advanced attacks can be regarded as phased progressions, but individual attack phases may be bypassed, occur more than once or occur out of sequence. Raising resilience against the phased progressions of advanced attackers is possible by developing a layered defense strategy that aligns with an organization's threat model by adopting the assume breach and defense in depth principles.

Organizations and societies as a whole are becoming increasingly dependent on Information and Communication Technology (ICT). In lieu of an effective global cyber governance structure or effective deterrents, cyber attacks can be highly effective methods for APTs to achieve their socio-technical objectives towards strategic goals and are thus expected to increase in number and in force. Attack models such as the Unified Kill Chain could prove to be valuable to decelerate this trend, by allowing the structured analysis and comparison of past cyber attacks and by providing a solid basis to develop (or realign) defensive strategies to raise resilience against cyber attacks in the future.

6 References

[1] P. Pols, "Modeling Fancy Bear Cyber Attacks: Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks," 07-Dec-2017. [Online]. Available: https://hdl.handle.net/1887/64569. [Accessed: 05-May-2021].

[2] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Lead. Issues Inf. Warf. Secur. Res.*, vol. 1, p. 80, 2011.

[3] G. Engel, "Deconstructing The Cyber Kill Chain," *Dark Reading*. [Online]. Available: http://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542. [Accessed: 27-Apr-2017].

[4] "CSRC - Glossary." [Online]. Available: https://beta.csrc.nist.gov/Glossary/?term=2856. [Accessed: 05-Jul-2017].

[5] B. E. Strom *et al.*, "Finding Cyber Threats with ATT&CK™-Based Analytics," 2017.

[6] M. Laliberte, "A Twist On The Cyber Kill Chain: Defending Against A JavaScript Malware Attack," *Dark Reading*. [Online]. Available: http://www.darkreading.com/attacks-breaches/a-twist-on-the-cyber-kill-chain-defending-against-a-javascript-malware-attack/a/d-id/1326952. [Accessed: 09-May-2017].

[7] C. Nachreiner, "Kill Chain 3.0: Update the cyber kill chain for better defense," *Help Net Security*, 10-Feb-2015. [Online]. Available: https://www.helpnetsecurity.com/2015/02/10/kill-chain-30-update-the-cyber-kill-chain-for-better-defense/. [Accessed: 10-May-2017].

[8] B. D. Bryant and H. Saiedian, "A novel kill-chain framework for remote security log analysis with SIEM software," *Comput. Secur.*, vol. 67, no. Supplement C, pp. 198–210, Jun. 2017.

[9] S. Malone, "Using an expanded cyber kill chain model to increase attack resiliency," *BlackHat USA*, 09-Mar-2016. [Online]. Available: https://www.blackhat.com/docs/us-16/materials/us-16-Malone-Using-An-Expanded-Cyber-Kill-Chain-Model-To-Increase-Attack-Resiliency.pdf. [Accessed: 10-May-2017].

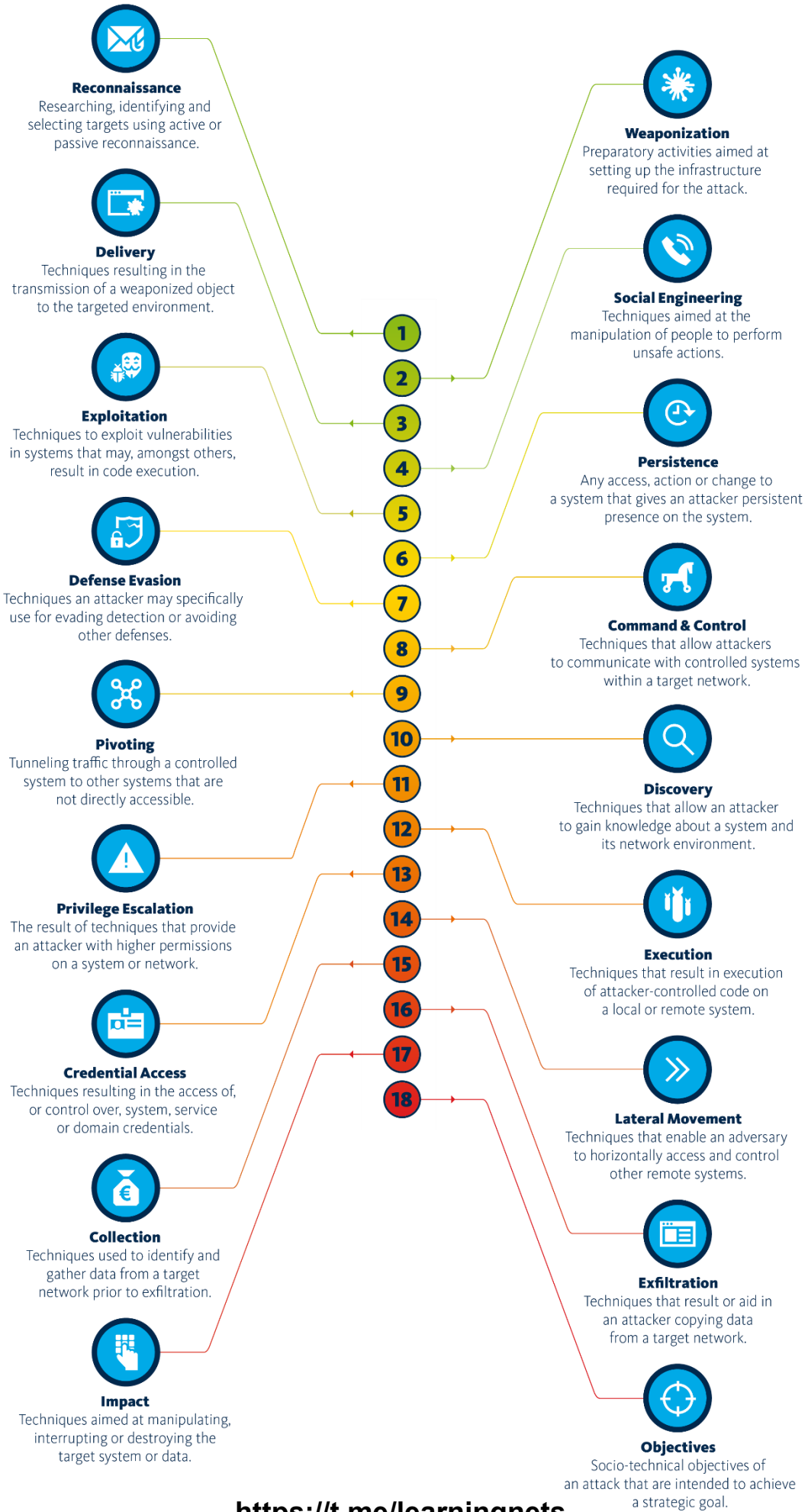
[10] C. J. Rogers, "Strategy, Operational Design, and Tactics."

[11] Defense Technical Information Center (DTIC), "Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms, As Amended Through 15 June 2015," Jun. 2015.

[12] A.-S. K. Pathan, *Securing Cyber-Physical Systems*. CRC Press, 2015.

7 Glossary

- **APT**: Advanced Persistent Threat
- **ATT&CK**: MITRE's Adversarial Tactics, Techniques & Common Knowledge framework
- **Attack vector**: a path or means to gain access to a computer or network
- **CKC**: Lockheed Martin's Cyber Kill Chain® attack model
- **Cyber**: socio-technical interactions between people and systems
- **Cyberspace**: a realm that consists of three interdependent layers
- **End-to-end**: the entire chain of events that is required to perform a successful attack
- **Foothold**: a position that can be used as a base for further advance
- **KC**: a kill chain, or a chain of events described on the tactical level of abstraction
- **Kill Chain**: a chain of events described on the tactical level of abstraction
- **MO**: modus operandi, or a distinct pattern of operation that is common to an actor (¶1)
- **Phase**: phase of an attack, or an attack tactic in its ordered arrangement
- **Procedure**: standard and detailed steps to perform a specific operational activity
- **Red Team**: a group of ethical hackers that performs threat emulations
- **Risk**: the potential that a negative impact occurs
- **Socio-technical**: layer in the cyberspace model comprising cyber interactions
- **Stage**: a step in the delivery process of attacker controlled code
- **Tactic**: tactical activities that are directed to achieve the objectives on an attack
- **Technique**: a non-prescriptive operational method to perform an activity
- **Threat**: potential cause of an unwanted incident that can affect an asset
- **Threat Actor**: an agent with (malicious) intent towards an asset that causes a threat
- **TTPs**: Tactics, Techniques and Procedures
- **UKC**: Unified Kill Chain, as presented in this white paper
- **Unified Kill Chain**: an end-to-end attack model for APT attacks
- **Vulnerability**: a weakness in an asset that can be exploited by a threat



UnifiedKillChain.com