Practical Cyber Security for Cyber Security Practitioners

Prof. Sandeep Kumar Shukla

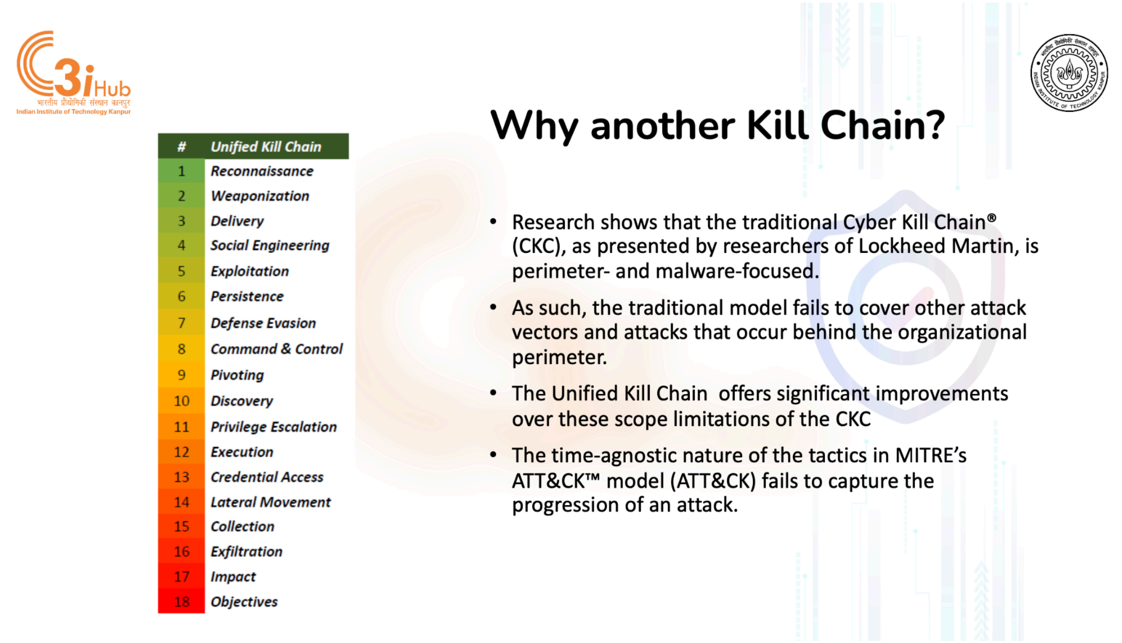
Department of Computer Science and Engineering

Indian Institute of Technology, Kanpur

Lecture 13

Deep Dive into Unified Kill Chain - Part 1

We will go now for UKC. We discussed cyber resilience yesterday. Now we'll see before UKC, we discussed the Lockheed Martin CKC chain and the MITRE ATT&CK. And now we come up with the UKC Unified Kill Chain.



Why another Kill Chain?

#	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

- 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
- The time-agnostic nature of the tactics in MITRE's ATT&CK™ model (ATT&CK) fails to capture the progression of an attack.

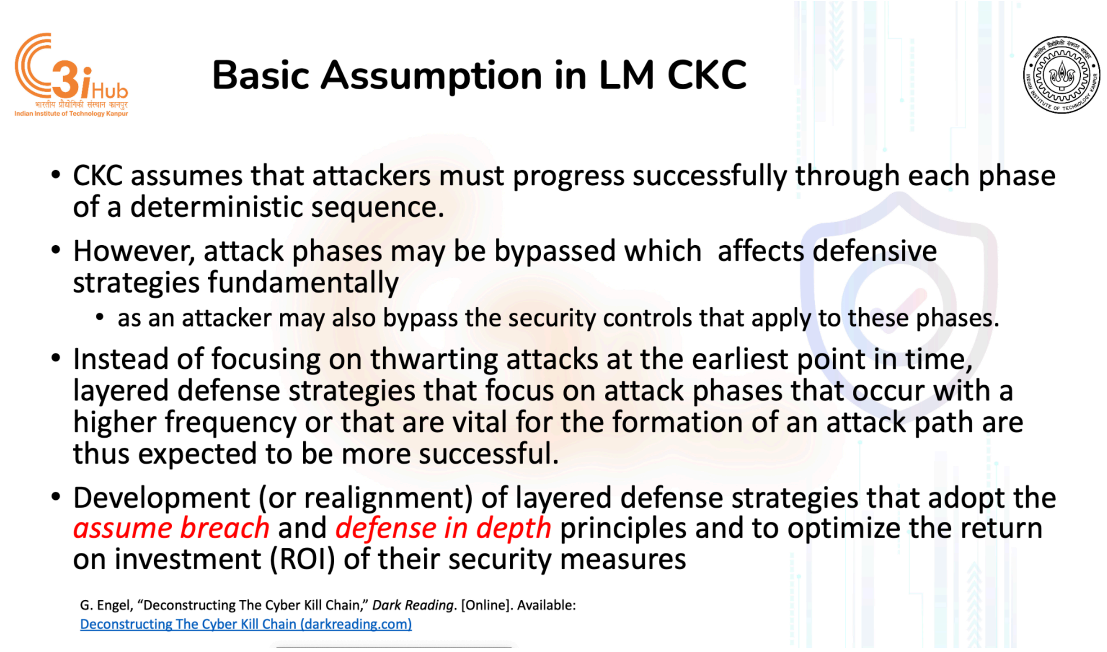
So Lockheed Martin CKC, LM CKC, when we see these all seven stages which we discussed, were criticized by this UKC by mentioning that this is more towards perimeter oriented or malware focused. Means, the activity or the attacker's motives were mentioned in the LM CKC were more limited towards the victim parameter like the victim organization. Once they enter into the victim machine or start recognizing and interacting with the victim infrastructure or the network, then it starts listing the behaviors like reconnaissance and initial access or exploitation, development, weaponization. But what they believe is that in the MITRE attack they already mentioned that there are many kinds of preparation like resource development and the other reconnaissance methods which attackers do before interacting with the perimeter of the victim. Okay, also the stages, all seven stages which mentioned in the LM CKC were more like if malware payload is going there, they are doing something, then it will get as a behavior like the weaponization is also towards developing the malware, exploitation is also towards executing the malware.

So this Lockheed Martin is kind of more towards - subset of what exactly happens in the whole attack picture. They don't consider the pre-attack scenarios and even not the post-attack scenarios. Here in this UKC, MITRE ATT&CK somehow they considered this pre-attack scenario. This UKC add-on is on top of the layer of this LM CKC and MITRE ATT&CK by mentioning 18 stages, attack stages. And also they add on a more one more thing like LM CKC they were based on that this stage will once weaponization happen then exploitation will execute.

Once exploitation happens then the privilege collection or whatever next stage is there that will get executed. There are dependencies between these stages. What UKC represents is that it should not be the case even in the real time. Attackers may not persist once they exploit the victim infrastructure, they may directly go with the command and control connection. So it should not be fixed that the attacker is going to do this action then only it will proceed ahead.

So what this UKC says is that the attacker may bypass some of the stages or the attacker may perform some of the set of actions repeatedly in a cyclic manner. So such insights have been included in this UKC framework. Okay, so after seeing this, we should not think like LM CKC and MITRE ATT & CK are not contributing to this. They already have their own existence and that can be used. One can use this LM CKC, even MITRE ATT&CK, even the blend of these multiple techniques out of these three for specific to the user's cases.

Also, yeah, we can see here that traditional models like LM CKC fail to cover the attack vectors or attacks that occur behind the organizational parameter. And these limitations and this sequence of step execution connecting the dots with the sequence and emphasizing that this one of these tests can be bypassed and can there be a cyclic manner of this behavior is the main contribution of a unified kill chain. So we will see all the stages one by one in later slides. Even with the MITRE ATT&CK, we did not see any progression of ATT&CK like behavior sequencing in the ATT&CK framework. There are lists of tactics but there is no sequence and there is no assumption that which will come after what.



Basic Assumption in LM CKC

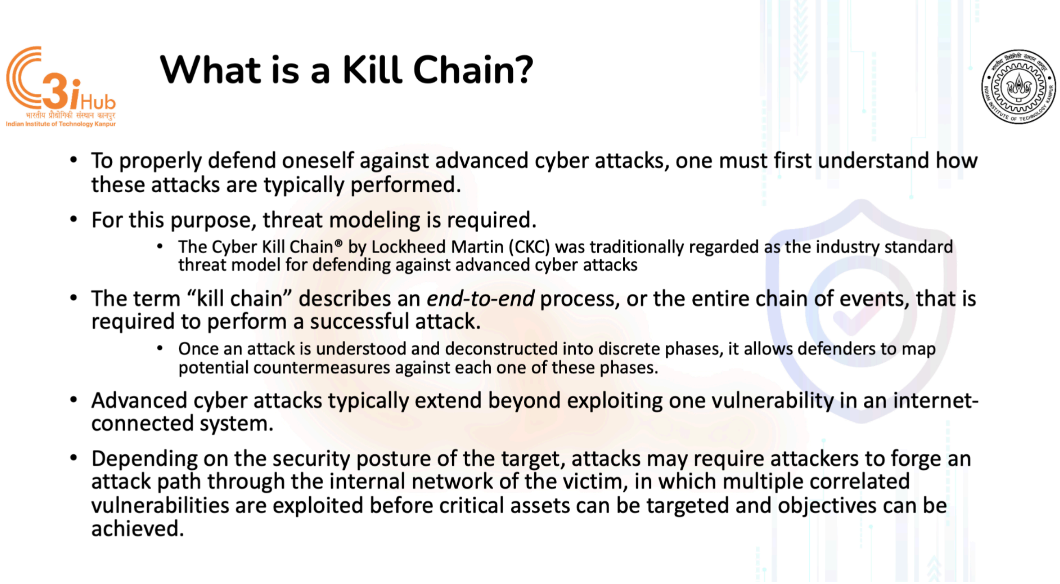
- CKC assumes that attackers must progress successfully through each phase of a deterministic sequence.
- However, attack phases may be bypassed which affects defensive strategies fundamentally
  - as an attacker may also bypass the security controls that apply to these phases.
- Instead of focusing 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.
- 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

G. Engel, "Deconstructing The Cyber Kill Chain," *Dark Reading*. [Online]. Available: Deconstructing The Cyber Kill Chain (darkreading.com)

Online read: https://www.darkreading.com/cyberattacks-data-breaches/deconstructing-the-cyber-kill-chain

So as we discussed, CKC assumes that an attacker must progress successfully through each phase of a deterministic sequence. Like one should be completed, then it gets proceed ahead for the another phase. However, these phases can be bypassed, which UKC mentioned. And an attacker may also bypass the security controls to apply these phases, obviously. So instead of focusing these attacks at the earliest point in time, this layer defense that focuses on attack phases which occurs with the higher frequency will be vital for the information of the attack path that is thus expected to be more successful.

What we are trying to say here is that rather than focusing on the all set of attack phases, this defense mechanism which we are implementing at our end, we can focus on the only attack phases which are occurring very frequently like command and control connection. This mostly happens for every sophisticated attack because that payload is going to communicate with the CNC server. So, this can be prioritized based on this attack phase analysis which is occurring with the higher frequency. Also one can develop this layered defense strategy by adopting this assuming bridge like we are assuming that bridge will happen and defense in depth like multiplying multiple security measures rather than relying on only one security measure. One has to rely on this set of security measures to have faith that if one gets compromised, the other one will combat the attack. So using methods like assuming the breach and following the defense in depth, one can go with implementing the layer defense strategy in the organization.

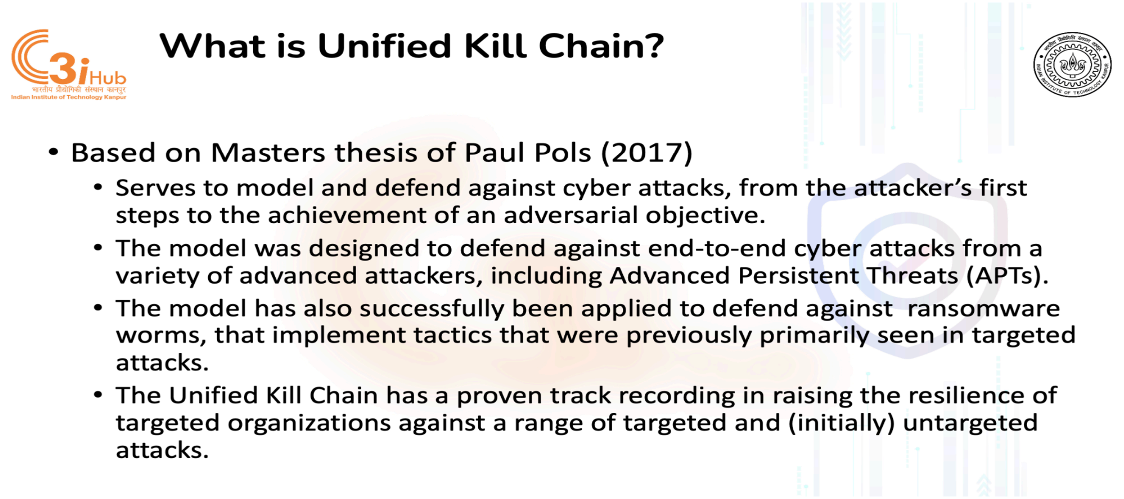


What is a Kill Chain?

- 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.
  - The Cyber Kill Chain® by Lockheed Martin (CKC) was traditionally regarded as the industry standard threat model for defending against advanced cyber attacks
- The term “kill chain” describes an *end-to-end* process, 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.
- 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.

So we'll see what exactly the kill chain is. So to defend oneself against advanced cyber attack, one must have to understand first that these attacks are typical, how these attacks are typically performed, which is what kill chain represents. For this, LM CKC, which we already studied in the past classes, we have to model the threats, how it is proceeding and what exactly the attack flow is, and what the usual attack flow is. Then the skill chain describes the end-to-end process which includes the entire chain of events which attackers follow to perform a successful attack.

Then once an attack is understood, once we understand the attack flow, Then we have to deconstruct these all phases and which allow us to understand the defensive mechanism mapping these potential countermeasures against each of these phases so that we can place these countermeasures according to these attack phases in the kill chain. Yeah, depending on the security posture of the target of the victim infrastructure attacker may require to forge an attack path through the internal network of the victim in which the multiple correlated vulnerability may get exploited before any critical assets they target.

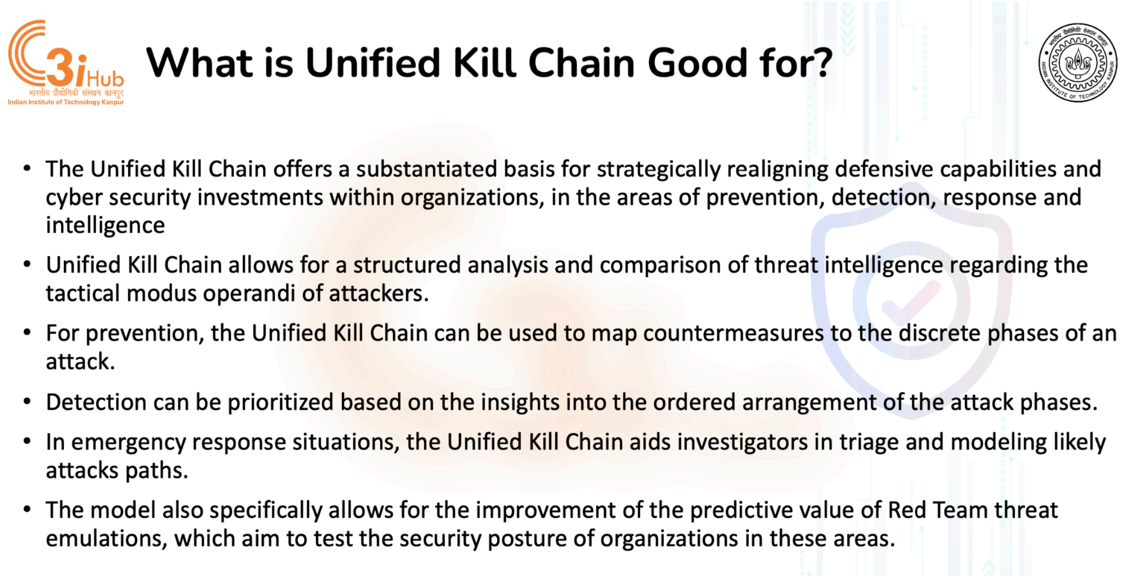


What is Unified Kill Chain?

- Based on Masters thesis of Paul Pols (2017)
  - Serves 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 Advanced Persistent Threats (APTs).
  - The model has also successfully been applied to defend against ransomware worms, that implement tactics that were previously primarily seen in targeted attacks.
  - 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.

So now we'll see what exactly this unified kill chain is. This is a master thesis of Paul Scholes. He has done this analysis and presented this framework as his master thesis. This UKC serves to model and defend against the cyber attacks from the first step of the achievement to the adversarial objective, like from the starting steps to the, till it is gaining its objective, it remaps all of these phases. Also, this is more suitable or more proposed, specific to these advanced attackers like advanced persistent threats. This model has also applied a defense against ransomware, which they have explained in his thesis, which implements tactics that were previously primarily seen in the targeted attacks. Also this has a proven track recording and raising resilience which we discussed yesterday of the targeted organization against any range of targeted or untargeted attacks.

So we need to first understand what exactly this UKC is good for.

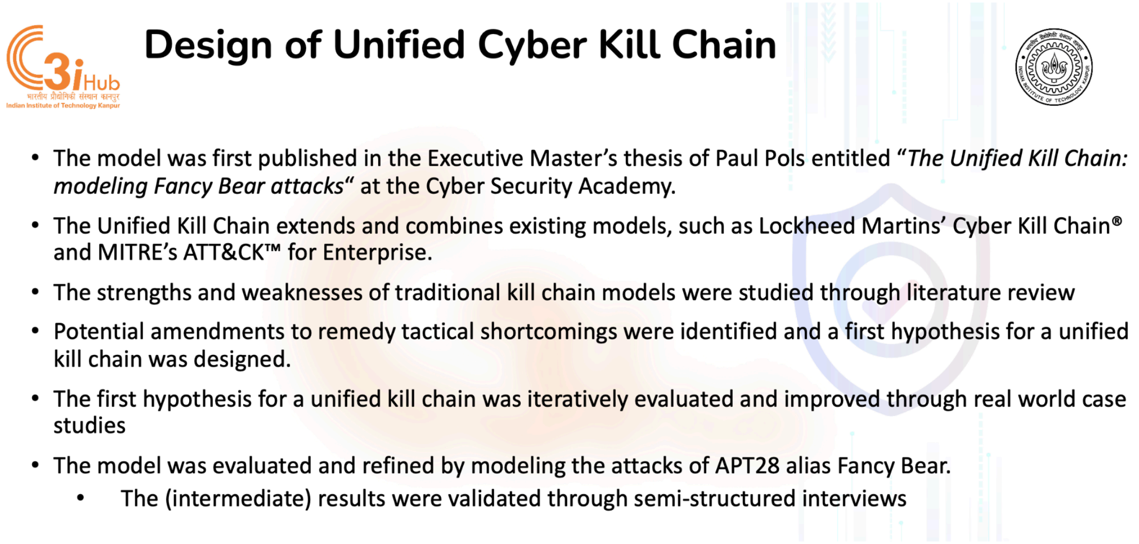


What is Unified Kill Chain Good for?

- 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
- Unified Kill Chain allows for a structured analysis and comparison of threat intelligence regarding the tactical modus operandi of attackers.
- For 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.

As it offers the strategically realigning the defensive capabilities based on the attack phases which it is listing like all 18 attack phases. See, this helps in preventing, detecting and even the response and intelligence. This allows structured analysis. If you have a structured way to have progression of the attack, one can perform a structure analysis and aids in comparison of the threat intelligence regarding the tactical modus operandi of the attackers. For prevention perspective, the UKC can also be used to map the countermeasure for each of these attack phases.

With the detection point of view, this can be prioritized based on the insights into the ordered arrangement of the attack phases, how it has been arranged. And also as an emergency response in the emergency response situation, this can also aid investigators in triage and modeling likely attack paths, what exactly attack paths were followed during the attack. This also allows for an improvement in the predictive value of rate of threat, in which they usually perform a set of actions to measure the security posture of the organization.



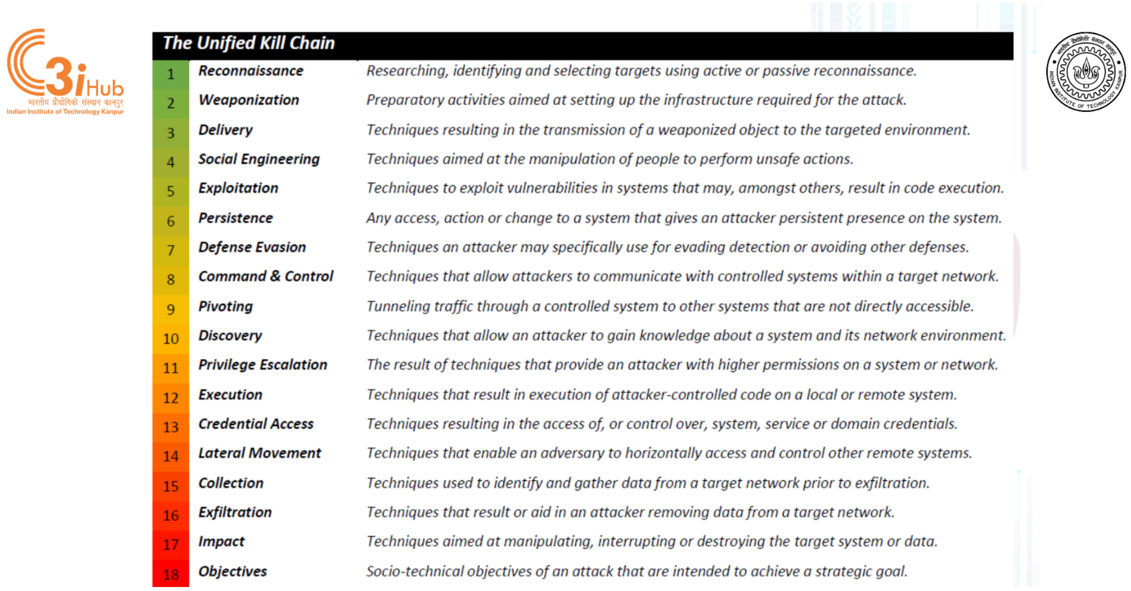
Design of Unified Cyber Kill Chain

- 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.
- The Unified Kill Chain extends and combines existing models, such as Lockheed Martins' Cyber Kill Chain® and MITRE's ATT&CK™ for Enterprise.
- The strengths and weaknesses of traditional kill chain models were studied through literature review
- 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 model was evaluated and refined by modeling the attacks of APT28 alias Fancy Bear.
  - The (intermediate) results were validated through semi-structured interviews

So altogether, we have seen several pros of the UKC with the perspective detection prevention response. Now their master thesis has a detailed case study on this fancy bear attack, how they use this UKC to model these fancy bear attacks.

Online read: https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf

They also like they mentioned that they are extending and combining the existing capabilities LM CKC and MITRE ATT&CK. So if you go through all 18 stages, these are nothing but the combination of LM CKC and the MITRE ATT&CK tactics. They have studied their weaknesses and strengths of both LM CKC and MITRE ATT&CK in their literature review of the thesis. They have these potential amendments to remedy, tactical shortcomings were identified and they first hypothesize that you can see an idea, giving a framework which measures the progress or list the sequence of attack phases. And then they have evaluated it with some different case studies which they have mentioned in detail in their thesis.



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.

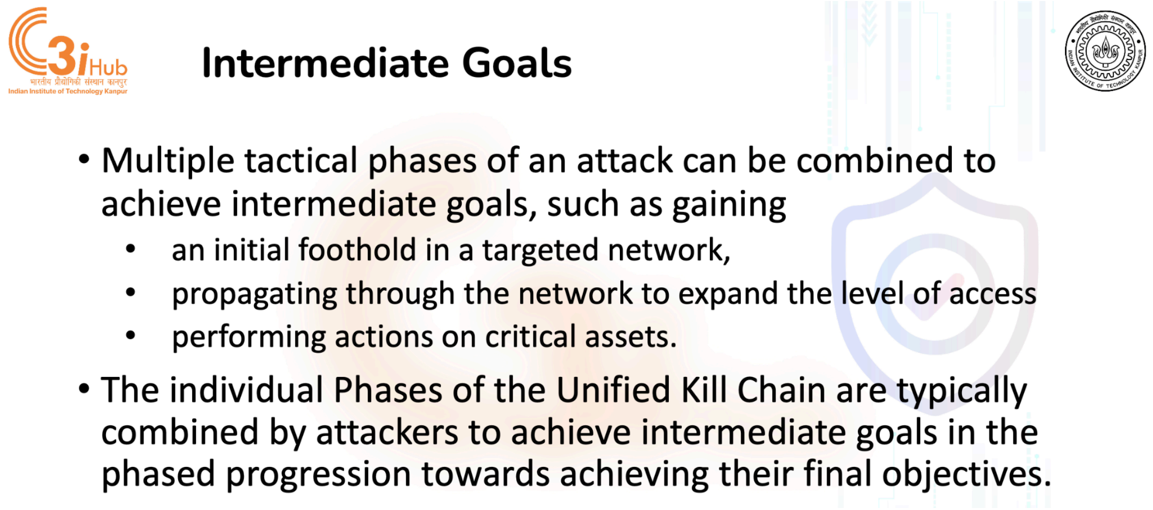
So this is available online on their website, UKC, unifiedcyberkillchain.com, I guess. So we'll see these attack stages one by one. First one is reconnaissance, which includes the activity related to researching, identifying, and selecting targets, either using active or passive communication. Weaponization, this part comes from LM CKC where they prepare the activities and create the infrastructure to do the attack.

In the delivery, they deliver the weaponized object or the payload. In social engineering, they will trick and find a social way to reach out to the victim and deliver their code. In the exploitation, they will exploit the vulnerability if there is existing in the system. or they execute the code, deliver malicious code. In the persistence, they will gain the persistent access of the victim machine. In the defensive evasion, they'll try to evade detection and other defense mechanisms.

In command and control, they will communicate with the control system like attackers, control systems which attackers control. Then in pivoting, this is a key stage which has not been seen previously, pivoting. This is tunneling the traffic through a kind of control system to other systems that are not directly accessible. So what happens when any attacks happen, sophisticated attackers, they compromise one machine, they will tunnel that machine and try to move towards the different machine by keeping that machine as a base.

So there this pivoting phase comes in. So the first machine which was initially compromised and which let other machines to get compromised, this activity comes under the pivoting. because this pivoting also gives a rise of cycling activities. Like once attackers came to one machine, they make a C2 communication, they do some action like persistence or privilege escalation or other activities, then they will repeat the same, there is a chance that they will repeat the same or at least set of the activities on the other machine on which they will again, they will make the target in the same network by pivoting the first machine. Then the next is discovery in which they'll discover the available machines or network environment or the compromised machine.

Then privilege escalation, then execution. This all means the same which we referred to in the MITRE ATT&CK framework, either in this or the LM CKC. Then credential access will happen, lateral movement, collection, exfiltration, impact and objective. So this impact represents the techniques which aim to manipulate or interrupt or destroy this targeted system or data. In the objective, they will achieve the socio-technical objective of an attack that is intended to achieve the strategic goal. So mostly sophisticated or targeted attacks, they arise with some kind of socio-technical objectives or even the political also.

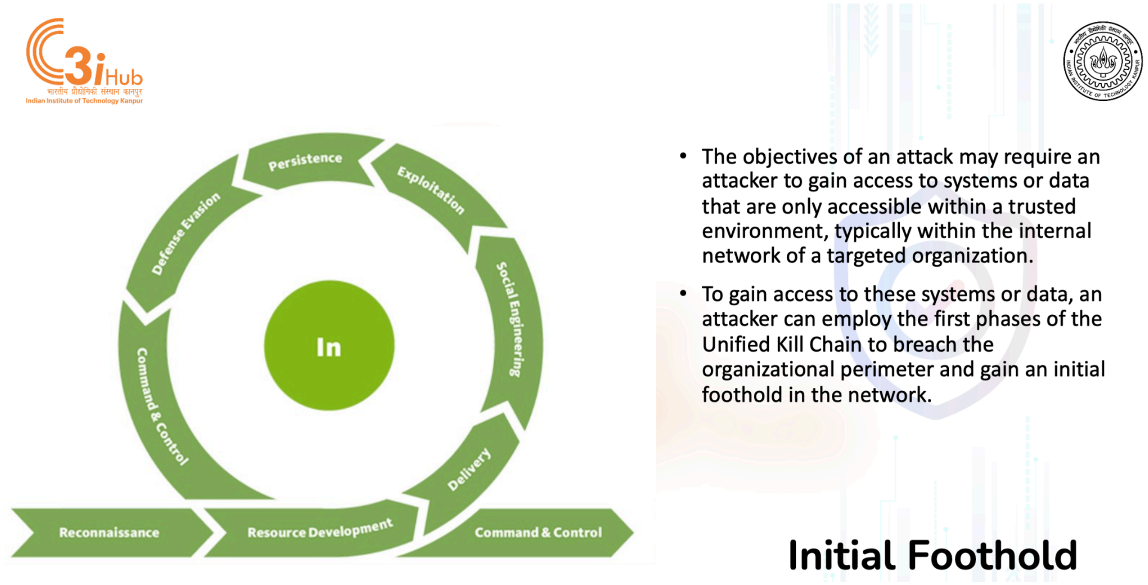


Intermediate Goals

- 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
  - performing actions on critical assets.
- 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.

Now in this whole 18 attack phases there are some intermediate goals which you can see have mentioned that attackers try to achieve. There are multiple tactical phases of an attack which can be combined to achieve an intermediate goal. such as gaining an initial foothold in a targeted network. The first foothold how they get into the system and make their foothold in the network that can be a kind of one intermediate goal of the whole attack. The second one can be propagating through the network or expanding the level of access.

Once they have an initial foothold they will try to propagate in the whole network that comes under the second intermediate goal. In the third one, they perform actions on the critical assets. Once they find the critical assets, they will start performing actions based on their objective. This kind of three different goals or mini goals you can say, they divided and these all 18 phases were divided into these three intermediate goals. So we will see them one by one in the further slides. The unified phases of the UKC typically combines the attackers to achieve the intermediate goal which I just explained in the phase progression towards achieving the final objective.



- 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.

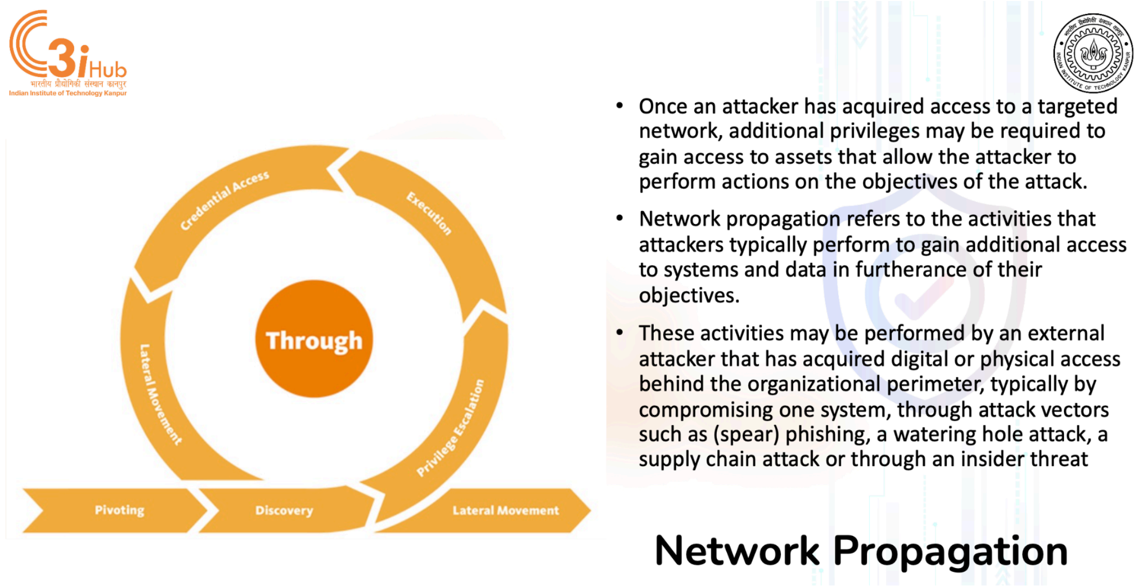
Initial Foothold

So this is the first one, the initial foothold compromise system. So this is the first intermediate goal in which the attacker will try to get the initial foothold in the victim network. So the phases that come under this intermediate goal are reconnaissance, weaponization, then delivery, then social engineering, exploitation, persistence, defensive evasion, command and control. attack objective or attack phases you can say attackers follow on the initial foothold machine on the initial targeted machine which they compromised or compromised machine and they perform all this action once they made this command and control connection.

Now they will start pivoting this machine and going forward for the other looking for the other available assets or the machines in the network. So as I said earlier, after delivery, there may be a chance that the attacker may not follow social engineering. They can directly go to the exploitation. Then delivery may contain any zero-day vulnerability or something which can directly exploit the machine. And in that case, one may not persist and they directly go to the defense evasion and or they may ignore this persistent defensive evasion both and directly make the command and control connection.

So this is the flexibility which UKC represents in their framework. So here the objective of an attacker may require an attacker to gain access to the system or data that are only accessible with the trusted environment typically within the internal network or target environment. Once they are here they can go within the network systems and data which were only accessible with the trusted environment. So this machine which they compromise is also a part of that network. Further to gain access to the system or data, an attacker can employ the first phase which we just discussed to bridge the organizational perimeter and gain the initial foothold.

The second intermediate goal is network propagation, like propagating inside the internal network in which they are already connected with.



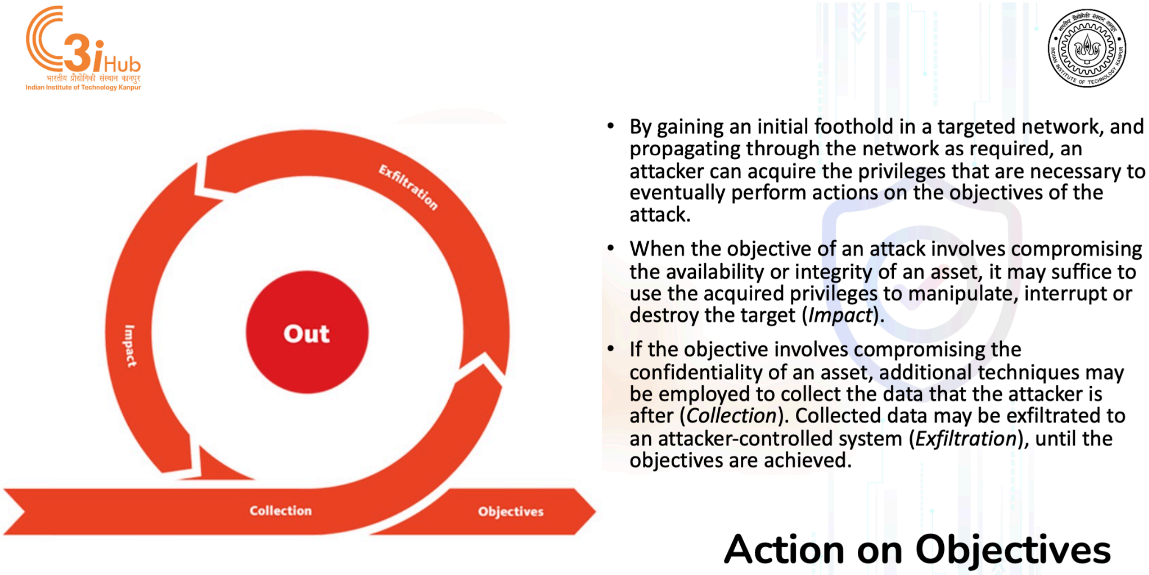
- Once an attacker has acquired access to a targeted network, additional privileges may be required to gain access to assets that allow the attacker to perform actions on the objectives of the attack.
- Network propagation refers to the activities that attackers typically perform to gain additional access 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

Network Propagation

This pivoting, after this pivoting they may discover, they may do this privilege escalation, they may do execution, they may do a credential access to gain the access of the other machine, they may do lateral movement once they found a way to get the access and then they may get the access okay. This may happen multiple times. The earlier one also this initial foothold may happen multiple times on the different machines. So assume they compromise one machine, they go to the other machine, they perform this action.

Now they will go to the third machine, they will perform this action. Similarly, they can propagate in the whole network. So this sequential propagation and emphasizing that this cyclic activity is usually being executed in the environment which has not been formalized or listed in any framework, so they represented that in this way. So once attackers have acquired access to the target network, they may perform additional privileges to get the privilege escalation or they may allow attackers to perform some other malicious actions once they escalate the privilege. This network propagation refers to the activities that attackers typically perform to gain additional access to the system or data in the furtherance of their objective. These activities may be performed by an external attacker that has acquired digital or physical access behind the organizational parameter which is obvious.

The attacker will be behind the organizational parameter typically either by compromising one system to any attack vector like spear phishing or watering hole attack or they may go with the supply chain or any insider threat also can get the access of the internal network to the attacker.

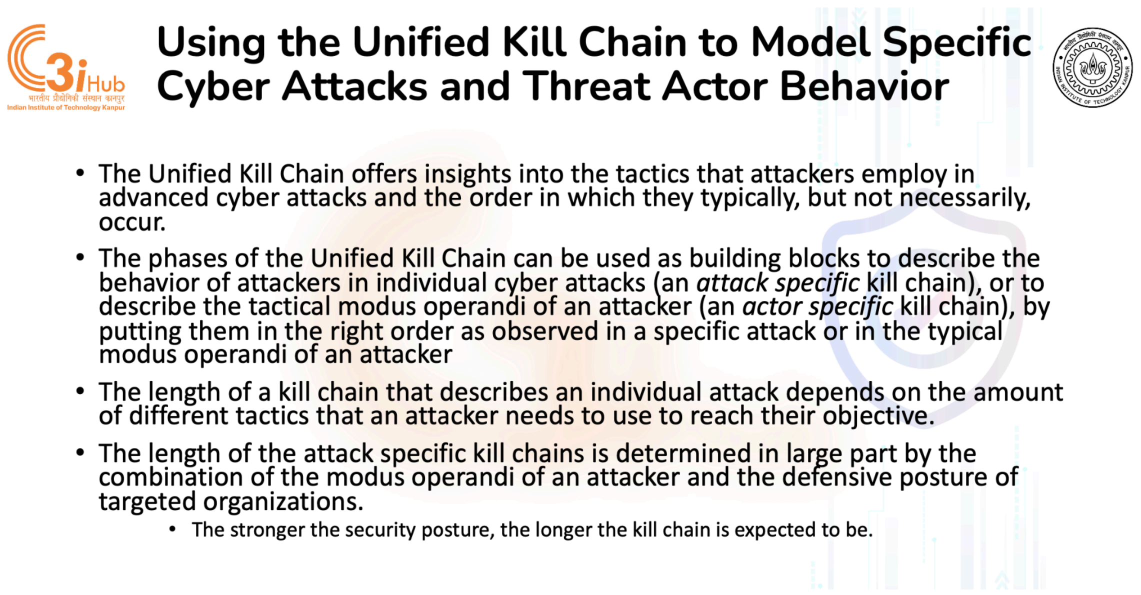


- By gaining an initial foothold in a targeted network, and propagating through the network as required, an attacker can acquire the privileges that are necessary to eventually perform actions on the objectives of the attack.
- When the objective of an attack involves compromising the availability or integrity of an asset, it may suffice to use the acquired privileges to manipulate, interrupt or destroy the target (*Impact*).
- 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.

Action on Objectives

Now we come to the final intermediate goal which was action on objective where attackers access the critical assets present in the victim infrastructure. Once they have the access of the critical asset they may collect those assets they may exfiltrate, then because of this collection and exfiltration there will be some impact based on what kind of activity they performed and they may achieve their objective. So this is the final intermediate goal of this UKC in which by gaining an initial foothold in a targeted network and after propagating through the internal network, attackers can acquire the privileges that are necessary for collecting these assets and eventually performing the actions on their objective. When the objective of an attacker involves compromising and availability and integrity of the assets, they may use the acquired privilege to manipulate or interrupt the data which will be reflected in this attack phase impact.

So if they want to compromise the integrity of the asset they may modify or manipulate the asset and that will be seen in this attack phase impact. Further if the objective involves compromising confidentiality. These attackers may employ the collect the data and they may exfiltrate this to the external network which will come considered this in the collection phase and the exfiltration will come in this phase exfiltration. So they will do this to achieve their objective.



Using the Unified Kill Chain to Model Specific Cyber Attacks and Threat Actor Behavior

- 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 of the Unified Kill Chain can 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 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.
- 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.

Now using this UKC model to any model specific cyber attacks and the threat actors behavior how we can use it.

So this UKC offers insights into the tactics of the attacker, like all 18 tactics which we discussed, which they employ in the sophisticated attacks, in the order in which we saw these cycles, but yeah, not necessarily that they will occur. All these 18 phases are not necessary to occur in any target attack. The phases of UKC can be used as a building block to describe behavior of attackers. So this can list if we have a set of attack phases which they followed map to this UKC framework one can understand the behavior of attacker how it behaves, how what exactly yeah the behavior of the attackers in any targeted attack or to describe their tactical models apparently of the attacker by putting them into the right order, this putting them in the sequence, in the sequence of form or the right, in the ordering, one can understand this what exactly and how they behave based on the, based on any targeted environment. Like if we have some set of defensive measures already placed or how they do this privilege escalation, how they do this persistent connection.

that this kind of analysis and referring them to as a mapping of what exactly the models render the attacker, this framework will be helpful. The length of the kill chain describes that individual attack depends on the amount of different tactics, which is like the total 18 we listed in this framework, which attackers need to use to reach their objective. Also this length of attack specific kill chain is determined in the larger part by the combining the modus operandi of the attackers and defensive posture of the targeted organization like I just discussed based on this defensive counter measures employed on the victim machine or victim infrastructure and the modus operandi which attacker has been employed in the whole attack scenario one can understand and determine the what how sophisticated it was and this sophistication depends on the how long kill chain they were able to make. So with the perspective of attackers, the sophistication depends the longer they make a kill chain, they are more sophisticated and from the victim perspective, we can say that they have a stronger security posture.Yes, so from the victim infrastructure, one can say that if they are trying to achieve this all track phases for a longer, like if they are not able to get the access of the critical assets quickly, so one can see that if longer the skill chain is for any specific attack, one can measure that the more stronger security posture we have in the victim organization.

Yes. Yes. Yes. Okay, so in the Lockheed Martin kill chain, cyber kill chain, they mentioned that breaking one stage will destroy the attack flow. Also in addition to that they mentioned that at this stage, this weaponization is required to get the, to do or perform the next attack stage. Here they are specifying that one stage is not dependent on the others even though we are making a sequence one can get bypassed plus they are giving a view and insights to be pivot on one machine and roaming towards another machine which has not been seen in earlier frameworks. So there is no sequencing or consideration in this, of this whole attack flow in the earlier framework, plus in this pivoting. There is no TTP or techniques specific to this pivoting in the MITRE ATT&CK, even though there is social engineering.

And these authors believe that social engineering is a kind of key to get the initial access and that should be as a different part rather than including that in their initial access. That is their perspective. That's why they kept social engineering as a different space. And this pivoting makes some kind of huge contribution in this framework, which gives a totally different way to see how these real attacks were progressing in the victim environment. This is not exactly the part of lateral movement because pivoting is the activity to get access to one system.

I am sitting here and then trying to get access to the others. Seeing what exactly lateral movement is there is another stage in this you can see there is a stage for lateral movement too. Lateral movement means I am going, I am going from one machine to another machine, then another to third and third to fourth. Pivoting means I am standing here and letting others, downloading other samples and sending them to get executed on the other machines. So it is kind of pivoting one place and roaming and seeing other systems or assets. Yes, I made a command control with that initial compromise machine and then I am letting my payload or executables to see and compromise other machines and collect information at one machine and give it to me.

See order will not fail, probably attack will get stopped but order will not fail, order they have seen is a kind of traditional or usual way to travel and do the attack. Yes. Obviously if you break the pivoting even so there is one more compromise machine and if it does not have access to critical assets this attack is stopped. There, I don't believe that they say that if we do not, if we break the one stage, it should not be like an attack will stop. Rather than MITRE, we're trying to just accumulate and list and create a knowledge base to what exactly and what all set of things attackers can do, that's it.

So they have not mentioned anything about breaking the stage or connecting the stages even. So, it is kind of them categorizing and cataloging all kinds of activities and attackers based on these tactics and inside these tactics there is a set of techniques. Can be if you have any different insights which these three are not addressing then obviously we can go with a different framework also which is giving more, adding more contribution towards giving some intelligence or giving some better analysis based on what we have.

These three are fixed. So all behavior, they categorize in three ways, that getting initial foothold, then network propagation, then action on objective. And then inside are all these three intermediate goals. Like tactics was also a mini goal, right? In Imitre, they divided 14 different goals. Similarly, they made three intermediate goals here, and inside these three intermediate goals, there are sub goals or sub stages or phases, you can say.