

Breaking the cyber kill chain by modelling resource costs

Blind Review¹

Anonymous Inc

Abstract. To combat cybercrime, a clearer understanding of the attacks and the offenders is necessary. When there is little available data about attack incidents, which is usually the case for new technology, one can make estimations about the necessary investments an offender would need to compromise the system. The next step would be to implement measures that increase these costs to a level that makes the attack unattractive. Our research method follows the principles of *design science*, where cycles of research activities are used to create artefacts intended to solve real-world problems. Our artefacts are an approach for creating a *resource costs model* (RCM) and an accompanying modelling tool implemented as a web application. These are used to find the required attacker resources at each stage of the cyber kill chain. End user feedback show that structured visualisation of the required resources would raise the awareness of the cyberthreat. This approach has its strength and provides best accuracy with specific attacks, but is more limited when there are many possible attack vectors of different types.

Keywords: cyber kill chain, costs, resources, profiling, attack tree

1 Introduction

As our use of technology in almost every aspect of life steadily increases, so does our exposure to cybercrime. To combat this growing form of criminality, a clearer understanding of the costs, benefits and attractiveness of cyberattacks is necessary [16]. This is in accordance with *Routine Active Theory* [5], extended to include cybercrime [6, 8], which states that crime will occur when all of the following four conditions are met: There exist an 1) *accessible and attractive target*, 2) *the absence of a capable guardian* and the presence of 3) *a motivated offender* with 4) *the resources required to commit the crime*. For the latter case, it is not just a question of technical skills, but also a requirement that the offender is able to invest in software development and hardware acquisition, as well as the time it takes to plan, prepare and perform the attack. Alternatively, the offender could bribe an insider or hire someone else to do it through cybercrime-as-a-service [19] being offered by third parties.

We hypothesize that during threat analysis, it is possible to reduce the complexity of the resource requirement to a monetary concern, complemented by a limited set of attacker characteristics. This will allow us to identify the potential

offenders and come up with technical and non-technical mitigations that will significantly increase the attacker costs.

The contribution of this paper is a modelling approach that maps resource costs to each stage of a cyberattack, and derives the total costs of the attack. We have utilized principles from Schneier’s *attack trees* [30] and the Lockheed Martin’s *cyber kill chain* [11], both already widely known in the security community, to structure this approach. A dedicated prototype tool has been developed to simplify and visualise this process, and we have completed the first rounds of iterative evaluation among experts. This tool is able to interactive show calculations and extract potential offenders based on a built-in library from available cyber-criminal profile literature. Our goal is to improve the accuracy of threat analysis, and especially increase the understanding and awareness of cyberthreats among sectorial domain stakeholders.

This paper is structured as follows. Section 2 gives an overview of background knowledge and literature, and Section 3 explains our method. Results are given in Section 4, which are discussed in the light of evaluations in Section 5. Finally, Section 6 concludes the paper.

2 Background

2.1 The cyber kill chain

Already in 1998, Meadows [21] presented a way of dividing attacks into different stages or phases to make visual representation easier. The next stage would not commence before the previous one had completed, and she used different colours to represent the assumed difficulty of each stage. The stages were not predetermined, but varied according to the nature of the attack. Later on, McQueen et al. [20] defined a set of five fixed stages, *reconnaissance*, *breach*, *penetrate*, *escalation* and *damage*, which were then modelled as a compromise graph in order to find the weakest link(s) in the attack path based on expected time-to-compromise. Hutchins et al. [12] describe different phase-based models from military usage (countering terrorist attacks) and the information security field (between 2008-2010), and present their own version nicked the *intrusion kill chain*. This model was later on renamed and branded as the *cyber kill chain* [11] by Lockheed Martin, and has proven to be widely popular among defenders of IT and enterprise networks [1]. The seven stages of the cyber kill chain are:

1. **Reconnaissance** - Research, identification and selection of target.
2. **Weaponization** - Coupling a malware (e.g. remote access trojan) with an exploit into a deliverable payload, e.g. a media file.
3. **Delivery** - Transmission of the weapon to the targeted environment, e.g. an email attachment or USB-drive.
4. **Exploitation** - Triggers malicious code. Ranges from vulnerabilities or auto-executing features in host’s operating system to users triggering execution.
5. **Installation** - Installation of the malware on the victim system, allowing the adversary to maintain presence inside the environment.

6. **Command and Control (C2)** - Establishes a channel for the adversary to access the target environment.
7. **Actions on Objectives** - Complete attack objectives, such as data extraction, break integrity or make system unavailable. Alternatively, establish a hop point to compromise additional systems.

As shown by Pols [25], there are many variants of the kill chain found in the literature. Some with different stage types and others with up to eighteen different stages. We chose to focus our work on the original seven stage cyber kill chain due to its popularity.

2.2 Attack tree cost modelling

Attack trees are acyclic graphs used to model threats from the viewpoint of the perpetrator. Schneier's original attack tree paper [30] showed how different costs could be assigned to alternative leaf nodes and how these propagated to define the cheapest way of attack. A fundamental paradigm for this kind of modelling is the assumption of a *rational attacker* [3], meaning that 1) *there will be no attack if the attack is unprofitable* and 2) *the attacker chooses the most profitable way of attacking*.

There have also been several approaches where costs are used in combination with other attributes. For instance, Buldas et al. [3] include costs, gains, penalties and associated probability values. Further examples of different attributes and references to papers that utilize costs in attack trees is given by Bagnato et al. [2]. Having more attributes enables additional ways of analysing attack trees, for instance Kumar et al. [17] show how to find the minimum time to complete an attack given a specific budget. Jensen et al. [13] present an approach where cost is a function of time instead of a constant cost per atomic attack attempt. Still, the major challenge of assigning accurate attribute values to attack tree nodes is difficult to overcome as attacker-specific information tends to be based on a best guess [29].

A comprehensive overview of more than thirty attack and defence modelling approaches based on directed acyclic graphs can be found in a survey paper by Kordy et al. [15]. A more recent survey focusing on fault and attack trees has been published by Nagaraju et al. [22].

2.3 Cybercriminal profiling

Shinder and Tittel [31] define a *profile* to be a set of characteristics likely to be shared by criminals who commit a certain type of crime. The use of profiles during criminal investigations can be traced several hundred years back in time, and though this is not an exact science, Nykodym et al. [23] argue that the track record legitimates the concept. However, they also argue that attackers have more advantages in a cyber setting as they do not have to be physically present at the crime scene.

The two main methods for profiling are known as *inductive* and *deductive* [34]. In the former, a profile database is developed based on information from already committed crime, and offender characteristics are correlated with types of crime. In the latter, forensics evidence is gathered from the crime scene and used to deduce the characteristics of the offender. Most of the established literature comes from the digital forensics field and relates to deductive profiling. We have been mostly interested in inductive profiling as a tool to identify potential offenders before any crime is actually committed. Furthermore, it is well established that likely offenders have a *motive, means* and *opportunity* (MMO) [33, 24] before committing any crime. As attacker costs belongs to the *means* characteristic, the literature becomes more limited. Warikoo et al. [34] have *capability factor* as one of their six profile identification metrics, where available resources for e.g. purchasing malware belongs. Preuß et al. [26] created a small set of profiles based on twelve cybercrime cases between 1998 and 2004. Due to the limited sample size, they could not create a structured set of attributes for these, but found that the principle of *minimum costs and maximum results* were present in all. Casey [4] presents a threat agent library of archetypal cybercriminal agents where *resources* is one of the eight attributes defining them. Casey’s work is used to define *Attack Resource Level* in the cyberthreat exchange format *STIX* [14].

3 Method

Our research method follows the principles of *design science*, supporting a pragmatic research paradigm where artefacts are created to solve real-world problems by cycling through research activities related to *relevance, design* and *rigor* [32, 9]. The problem we try to address is the challenge of quantifying cyberrisks when there is little reliable historical data about attacks. Our artefacts are 1) an approach for creating a *resource costs model* (RCM), that is used to find the required attacker investments at each stage of the cyber kill chain and 2) an accompanying modelling tool implemented as a web application.

As a part of the relevance cycle, we initially worked with opportunities and problems related to cybersecurity for maritime shipping. We analysed typical vulnerabilities and threats towards eNavigation systems, and made cost estimations for attacking the various underlying technology modules.

During the rigor cycle, past knowledge, as presented in Section 2, was examined and we chose to build on practices that already had a significant uptake among practitioners.

Most central to design science research is the design cycle, consisting of artefact construction, evaluation and refinements based on feedback. Initially, we applied “pen-and-paper” variants of the RCM and validated the expressiveness by constructing models of known cyberattacks towards maritime systems. The second iteration produced a *minimum viable product* (MVP) of the tool. Ries [27] defines a MVP as the version of a new product which allows developers to collect the maximum amount of validated learning about customers with the

least effort. Our MVP consisted of an info page tutorial and functionality for building basic resource costs models for each attack phase. For the evaluation we recruited eight security professionals who modelled a specific use case. These were observed during modelling and debriefed afterwards. The third iteration added the cybercriminal profiling feature, improved the user interface, as well as tweaking flawed features and functions.

4 Results

4.1 The resource costs model

In a *resource cost model* (RCM), each stage in the cyber kill chain represents the root node of a *resource tree*, depicted in Figure 1, which is similar in structure to an attack tree.

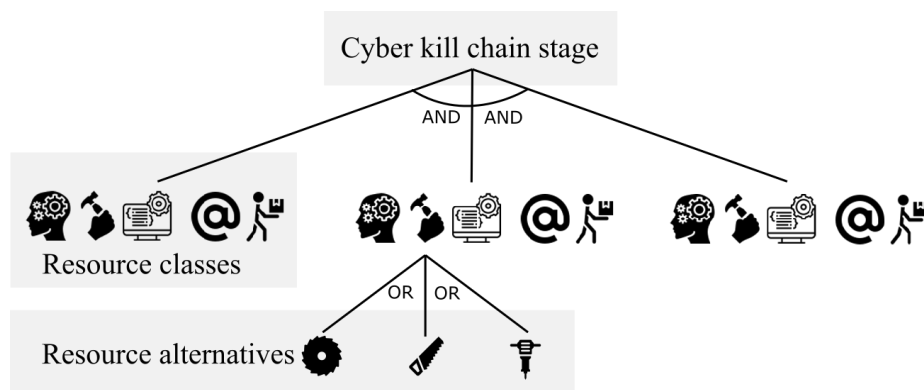






Fig. 1: A resource tree for a single cyber kill chain stage

The second level of the tree defines which resource types are required to complete the parent stage. At this level, all nodes have a conjunctive (*AND*) relationship since an attack would require all necessary resources. A resource can belong to five different classes:

-  **Skill:** Includes domain knowledge, malware development abilities or utilisation of cybercrime tools or guides.
-  **Tangible:** Necessary hardware components or other physical objects. This can range from advanced technology to soldering tools.
-  **Logic:** Commercially available software, data sets or cybercrime tools or services.
-  **Logic-atomic:** Necessary resources that can not be broken into smaller parts, e.g an IP-address, email address or a password.



Behavioral: Actions that must be conducted as a part of the attack, for instance bribing, sending out phishing emails or social engineering.

The third level in the tree, *resource alternatives*, are disjunctive (*OR*) leaf nodes that present ways to realize their parent resource class. Each resource alternative is associated with a cost interval and a confidence value. A confidence close to zero communicates that there is little evidence to support the stated cost interval. At the other end of the scale, a confidence of 1 means that there is exhaustive evidence to back the stated cost interval and that the price of the resource is not subject to great variation.

We can express the total cost interval of the attack T formally by stating that all resources R_j need to have a valid set V of resource alternatives. Let α represent the minimum estimated cost of the cheapest resource alternative and β represent maximum cost of the most expensive resource alternative. From this we can derive the following:

$$T = [(min\ cost = \sum_{\substack{stage \in \\ kill\ chain}} \sum_{i \in V} \alpha_i), (max\ cost = \sum_{\substack{stage \in \\ kill\ chain}} \sum_{i \in V} \beta_i)] \quad (1)$$

By letting ϕ be the average confidence of the n resource alternatives associated with a resource R_j and c_i is the confidence of a resource alternative i associated with R_j , we get the following associated confidence C of the total cost:

$$\phi_j = \frac{\sum_{i \in R_j} c_i}{n} \quad (2)$$

$$C = \prod_{\substack{stage \in \\ kill\ chain}} \prod_R \phi_j \quad (3)$$

In order to mitigate an attack, at least a one of the resources throughout the cyber kill chain must be made too expensive for the adversary. However, the adversary only needs a single resource alternative for each of the resources.

4.2 The IRCM tool

To validate the modelling approach, we have built an interactive installation of the model in the form of a web application called *Interactive Resource Cost Model* (IRCM) tool. This allows the users to model cyberattacks of their choosing, while concurrently deriving the total cost of the attack and probable cybercriminal profiles able to conduct it. An example screenshot from a single resource tree is shown in Figure 2, while a screenshot of the RCM for the complete cyber kill chain is included in Appendix A.



Fig. 2: A screenshot resource tree from the reconnaissance stage

These examples are taken from the maritime domain, where the *Electronic Chart Display and Information System* (ECDIS) is a central component for ship navigation. It displays the vessels position on a chart and integrates information from a number of sensors, such as radar, gyro, GNSS, echo sounder, weather measurements and the anti-collision systems. Malicious manipulation of this position could cause confusion on the ship bridge and potential course alteration could lead to collisions in congested waters [35]. The examples are loosely based on the demonstrated attack against an air-gapped ECDIS system by Lund et al. [18]. This attack was also structured according to the cyber kill chain, but in contrast to an external attack, it was conducted in cooperation with the Royal Norwegian Navy. Also, no information about resource costs were given, so here we have made our own estimations.

As can be seen in Figure 2, there are four resources defined for the reconnaissance stage. The first one, *ECDIS documentation*, is a tangible class, and the alternatives are to either *purchase* the documentation from the vendor legally, or *steal* it. The second resource is another tangible class, and represents an operational ECDIS unit that can be used to analyse its operating system, software and network traffic. It can be realized in different ways, by *purchasing a unit from vendor* or the *black market*, or running it as a software *simulation*. These alternatives vary in price, from relatively cheap software (where you pay according to sailing route) to more expensive hardware units in the range of \$10 000 - \$30 000. The third resource is of class logic-atomic, and represents information about the *ship inventory* used to determine which type and where the ECDIS units are installed. To simplify the model, only a single *bribe insider* alternative is used. The final resource is also of type skill, and represents required knowledge about *vulnerabilities* gained through *scanning and testing*.

Both resources and resource alternatives are created by using the tool input data forms. An example screenshot for the ECDIS resource alternative *purchased from vendor* is shown in Figure 3.

IRCM	Info	Attacker Profiles
Add a new resource alternative to ECDIS unit		
Name		
Purchase from vendor		
Description		
There is a wide range of dedicated ECDIS units available for purchase.		
Maximum cost:		
30000		
Minimum cost:		
10000		
Confidence:		
<i>(Where 0.1 indicates that you have no idea what the cost is and 1 indicates that you are sure of the cost, for example the cost of commercially available hardware)</i>		
0.9		
Motivation (number of hours):		
<i>(The time it will take an attacker to acquire or realize this resource alternative. As an example: How many hours will it take the attacker to develop a malware or to acquire a hardware component)</i>		
2		
Technical Skill:		
<i>(The academic and technical level an attacker must possess to be able to realize this resource alternative)</i>		
Minimal		
Legal Limit:		
<i>(Can the resource alternative be acquired or realized Legally or Illegally?)</i>		
Legally		
Access level:		
<i>(Does the resource alternative require Internal or External access level in order to be realized?)</i>		
External		
Create Alternative		
Technical skill levels		
None: The resource alternative require no expertise or training to be realized		
Minimal: The resource alternative can be realized through copying code and utilizing existing techniques and tools		
Operational: The resource alternative require an understanding of the underlying technology and methods used. The requirement to create a new attack or hacking tool falls into this category		
Adept: The resource alternative require an expertise in technology and attack methods to be realized.		

Fig. 3: A screenshot from the resource alternative window

The tool has a built-in database of cybercriminal profiles that the model inductively retrieves candidates from. This database is summarized in Appendix B and has been based on profile definitions we have found in the literature [34, 28, 4, 14]. We found out that mapping total attack cost with assumed *wealth* was not a very useful way of doing this. The wealthiest attacker is not always the most likely one, and attackers have more than one characterizing dimension. Therefore, the tool is able to exclude improbable attacker profiles from the database based on optional information that is assigned to the resources in the RCM. The exclusion rules are based on the following:

- Total minimal *cost* exceeds the financial capacities of the profile [*no cost, low, medium, high*].
- The accumulated time to require all resources exceed its *motivational* limit [*no time, low, medium, high*].
- Any resource alternative require a higher *technical skill* level than the profile possesses [*none, minimal, operational, adept*].
- Any resource that requires *moral limits* to be broken [*legally, illegally*].
- Any resource that require an *access level* the profile does not posses [*internal, external*].

The extended ECDIS attack example in Appendix A shows aggregated model information based on input contained in the individual resource tree for each attack stage. The cost interval has a broad range, mostly due to the choice of purchasing ECDIS hardware unit versus other cheaper alternatives in both the *reconnaissance* and *delivery* stages. Besides from these, the overall resource costs related to tangible and skill are relatively low. By analysing the model, we find that there are significant costs related to the *delivery* stage as the attacker would need physical presence at the ship and gain access to the bridge or bribe an insider. It is the air-gapping of the ECDIS that provides the main security measure by making delivery costly. When considering opening up for online software and chart updates, it is clear that additional secure measures will be needed to preserve an expensive attack vector. The confidence value is also very low, but would have been much higher if we had modelled the attack with a specific ECDIS unit in mind where costs are more certain. Also, a higher number of resources will automatically yield a lower confidence, which is natural since acquiring many resources increases uncertainty. The main benefit of the confidence is for attack comparison, which is not shown in these examples. Given the various exclusion rules that have been applied to the model, the most probable attacker profile in this case is *cyber warrior* (described in Appendix B).

5 Discussion

Hong and Kim [10] have pointed to the inherit challenge with graph-based attack models, namely the ability to scale. A purely tree-based model will generate large, bewildering attack trees for complex attacks. In turn, this creates a conflict between analysis and comprehensibility [7]. Hence, some sort of decomposition is needed. We chose to combine two modelling techniques to amplify their advantages and overcome some of their shortcomings. The cyber kill chain allows us to divide the attack into seven consecutive steps, and by stopping it in the early stages we don't have to embellish the later ones. The relatively small resource tree for each of the stages breaks down composite resource requirements into atomic ones, which can be more accurately estimated. This was the main takeaway from the first iteration of the design cycle. Secondly, we experienced that deriving a cost interval, rather than a single estimate, provides more confident information regarding the availability of an attack. A cheap, more available resource alternative set may provide a less stealthy attack than an expensive alternative. By determining both the minimum and maximum cost, we include both the risk willing and risk averse offenders. A large cost interval does not necessarily imply an inaccurate cost estimate, but rather that the evaluated attack can be carried out with a wide span of sophistication and possible impact on the target.

The second iteration involved expert end users who were observed using the MVP of the tool and debriefed afterwards. Seven out of these eight expressed that the main difficulty was to understand the difference between *resource* and *resource alternative* in the models. We were also able to observe that classifying

resources was not straightforward, and the users spent some time navigating between the information page and the modelling interface to check definitions and the tutorial example. Both of these issues improved quickly with hands-on experience and by refining the info page. It was stated during the debrief that “especially interesting is the fact that making only a single resource unavailable, thus breaking the kill chain, will mitigate the entire attack” and all independently agreed that the structured visualisation of the required resources would raise the awareness of the cyberthreat. Some also expressed that many of the resources are impossible to make unavailable, which is true of course. In the MVP, we used *attack trees* as the tree structure term, and this caused some confusion since the RCM focus on resource required to perform the attack and not the attack actions, hence we changed this to *resource tree*.

The third iteration has had a focus on inducing criminal profiles from the models. As already mentioned, the wealthiest attacker is not always the most likely one, therefore we are using five identifying attributes as exclusion rules. A known limitation is that none of these say much about the *motive* of the offender, that is *why* would she commit the crime. This has been out of our scope, but could be extended by looking at the attack impact and attacker reward. Those considerations would have to be determined on a case-by-case basis, requiring additional knowledge dimensions. There is a general criticism towards the cyber kill chain that it focuses too much on the perimeter and malware attack vector [25], and we have seen supportive evidence of that too. Therefore, future improvements could be to include other sets of stages more suitable to describe attacks such as for instance related to social engineering, denial-of-service or code injection.

6 Conclusion

Through the iterative nature of design science we have made many improvements to the RCM modelling approach and the accompanying tool. However, we still consider this work to be in progress with many potential improvements related to usefulness and usability. We are also planning to extend the user testing and evaluation, particularly in the field of maritime cybersecurity, but also in other domains to ensure that the artefacts could have a wider usage than just the maritime context. Nevertheless, there is no silver bullet to threat modelling. We are trying to address the real-world problem of missing historical incident data, which is a particular concern for new technology. The RCM has its strength and provides best accuracy with specific attacks; when there are few resources and resource alternatives. Hence, we would not recommend this approach when you want to represent attacks with many possible attack vectors of different types. In such cases, several RCMs could be created and compared, but this quickly becomes a tedious task. As always, the analyst should choose the right tool for the job at hand.

References

1. Assante, M.J., Lee, R.M.: The industrial control system cyber kill chain. SANS Institute InfoSec Reading Room **1** (2015)
2. Bagnato, A., Kordy, B., Meland, P.H., Schweitzer, P.: Attribute decoration of attack–defense trees. *International Journal of Secure Software Engineering (IJSSE)* **3**(2), 1–35 (2012)
3. Buldas, A., Laud, P., Priisalu, J., Saarepera, M., Willemson, J.: Rational choice of security measures via multi-parameter attack trees. In: *International Workshop on Critical Information Infrastructures Security*. pp. 235–248. Springer (2006)
4. Casey, T.: Threat agent library helps identify information security risks. Intel White Paper **2** (2007)
5. Cohoen, L.E., Felson, M.: Social change and crime rate trends: A routine activity approach. *American Sociological Review* **44**(4), 588–608 (1979)
6. Ekblom, P., Tiley, N.: Going equipped. *The British Journal of Criminology* **40**(3), 376–398 (2000)
7. Gadyatskaya, O., Trujillo-Rasua, R.: New directions in attack tree research: Catching up with industrial needs. In: *International Workshop on Graphical Models for Security*. pp. 115–126. Springer (2017)
8. Grabosky, P.N.: Virtual criminality: Old wine in new bottles? *Social and Legal Studies* **10**(2), 243–249 (2001)
9. Hevner, A., Chatterjee, S.: Design science research in information systems. In: *Design research in information systems*, pp. 9–22. Springer (2010)
10. Hong, J.B., Kim, D.S.: Performance analysis of scalable attack representation models. In: *IFIP International Information Security Conference*. pp. 330–343. Springer (2013)
11. Hutchins, E.M.: The cyber kill chain. Tech. rep., Lockheed Martin (2020), <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>, [Online; accessed 12-April-2020]
12. Hutchins, E.M., Cloppert, M.J., Amin, R.M.: Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research* **1**(1), 80 (2011)
13. Jensen, P.G., Larsen, K., Legay, A., Poulsen, D.: Quantitative evaluation of attack defense trees using stochastic timed automata. In: *International Workshop on Graphical Models for Security*. pp. 75–90. HAL Id: hal-01640091 (2017)
14. Jordan, B., Piazza, R., Wounder, J.: Stix version 2.0. part 1: Stix core concepts. Tech. rep., OASIS Committee Specifications 01 (2017), <http://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part1-stix-core.html>, [Online; accessed 13-April-2020]
15. Kordy, B., Piètre-Cambacédès, L., Schweitzer, P.: Dag-based attack and defense modeling: Don’t miss the forest for the attack trees. *Computer science review* **13**, 1–38 (2014)
16. Kshetri, N.: The simple economics of cybercrimes. *IEEE Security & Privacy* **4**(1), 33–39 (2006)
17. Kumar, R., Ruijters, E., Stoelinga, M.: Quantitative attack tree analysis via priced timed automata. In: *International Conference on Formal Modeling and Analysis of Timed Systems*. pp. 156–171. Springer (2015)
18. Lund, M.S., Hareide, O.S., Jøsok, Ø.: An attack on an integrated navigation system. *Nesesse* **3**(2), 149–163 (2018)
19. Manky, D.: Cybercrime as a service: a very modern business. *Computer Fraud & Security* **2013**(6), 9–13 (2013)

20. McQueen, M.A., Boyer, W.F., Flynn, M.A., Beitel, G.A.: Quantitative cyber risk reduction estimation methodology for a small scada control system. In: Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06). vol. 9, pp. 226–226. IEEE (2006)
21. Meadows, C.: A representation of protocol attacks for risk assessment. In: Proceedings of the DIMACS Workshop on Network Threats. pp. 1–10 (1998)
22. Nagaraju, V., Fiondella, L., Wandji, T.: A survey of fault and attack tree modeling and analysis for cyber risk management. In: 2017 IEEE International Symposium on Technologies for Homeland Security (HST). pp. 1–6. IEEE (2017)
23. Nykodym, N., Taylor, R., Vilela, J.: Criminal profiling and insider cyber crime. *Computer Law & Security Review* **21**(5), 408–414 (2005)
24. Pendse, S.G.: Ethical hazards: A motive, means, and opportunity approach to curbing corporate unethical behavior. *Journal of Business Ethics* **107**(3), 265–279 (2012)
25. Pols, P.: The unified kill chain: Designing a unified kill chain for analyzing, comparing and defending against cyber attacks. Cyber Security Academy (2017)
26. Preuß, J., Furnell, S.M., Papadaki, M.: Considering the potential of criminal profiling to combat hacking. *Journal in Computer Virology* **3**(2), 135–141 (2007)
27. Ries, E.: The lean startup : how constant innovation creates radically successful businesses. Portfolio Penguin (2011)
28. Rogers, M.K.: The psyche of cybercriminals: A psycho-social perspective. In: Cybercrimes: A multidisciplinary analysis, pp. 217–235. Springer (2011)
29. Saini, V., Duan, Q., Paruchuri, V.: Threat modeling using attack trees. *Journal of Computing Sciences in Colleges* **23**(4), 124–131 (2008)
30. Schneier, B.: Attack trees. *Dr. Dobb's journal* **24**(12), 21–29 (1999)
31. Shinder, D.L., Tittel, E.: Chapter 3 - understanding the people on the scene. In: Scene of the Cybercrime, pp. 93 – 146. Syngress, Burlington (2002)
32. Simon, H.A.: *The Sciences of the Artificial* (3rd Ed.). MIT Press, Cambridge, MA, USA (1996)
33. Van Ruitenbeek, E., Keefe, K., Sanders, W.H., Muehrcke, C.: Characterizing the behavior of cyber adversaries: The means, motive, and opportunity of cyberattacks. In: 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Supplemental (DSN 2010). pp. 17–18 (2010)
34. Warikoo, A.: Proposed methodology for cyber criminal profiling. *Information Security Journal: A Global Perspective* **23**(4-6), 172–178 (2014)
35. Wingrove, M.: Security flaws open ECDIS to cyber crime. Tech. rep., Riviera (2018), <https://www.rivieramm.com/opinion/opinion/security-flaws-open-ecdis-to-cyber-crime-24334>, [Online; accessed 20-April-2020]

A Tool screenshots

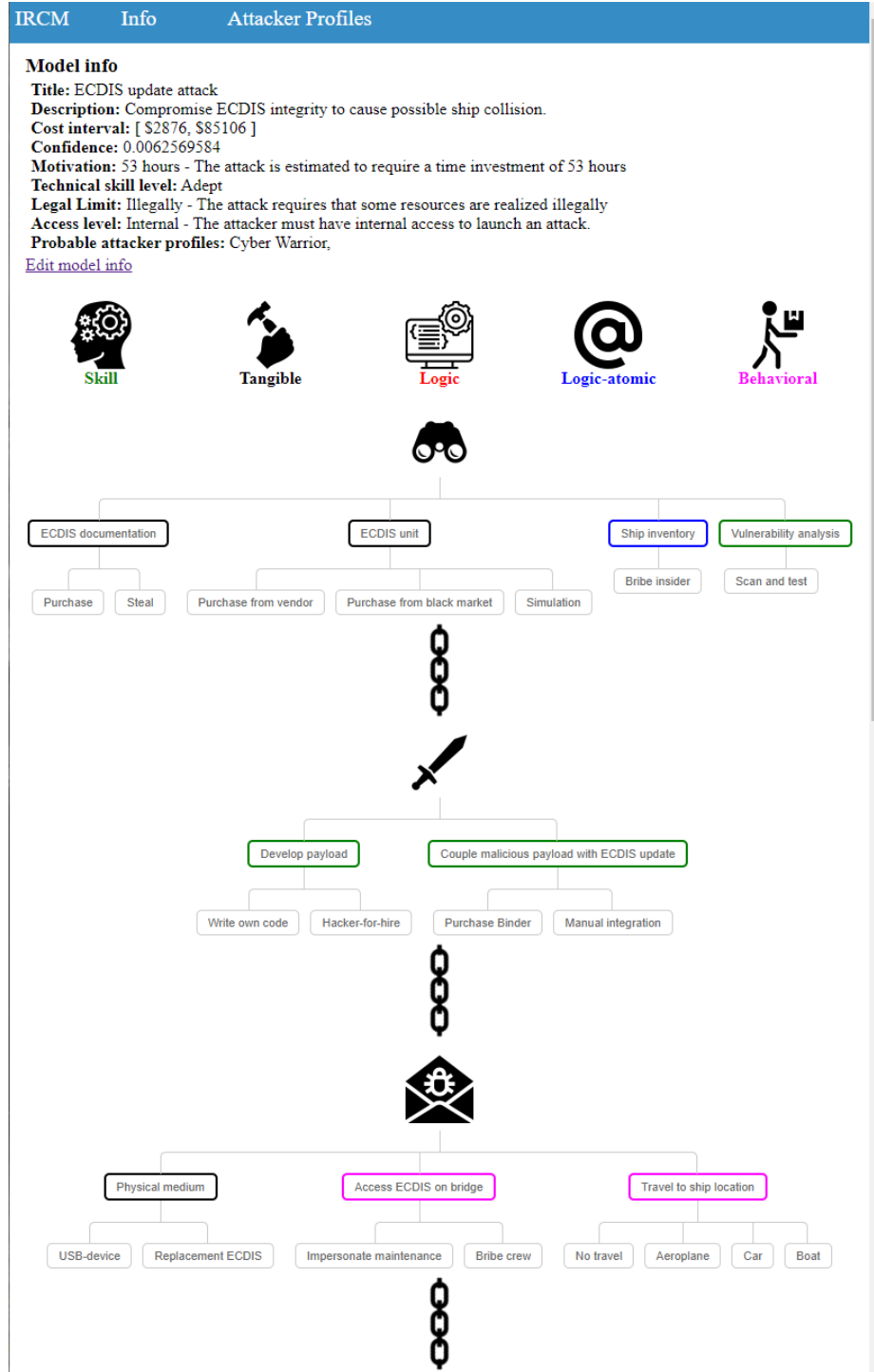


Fig. 4: A screenshot from the first three stages; *Reconnaissance*, *Weaponization* and *Delivery*.

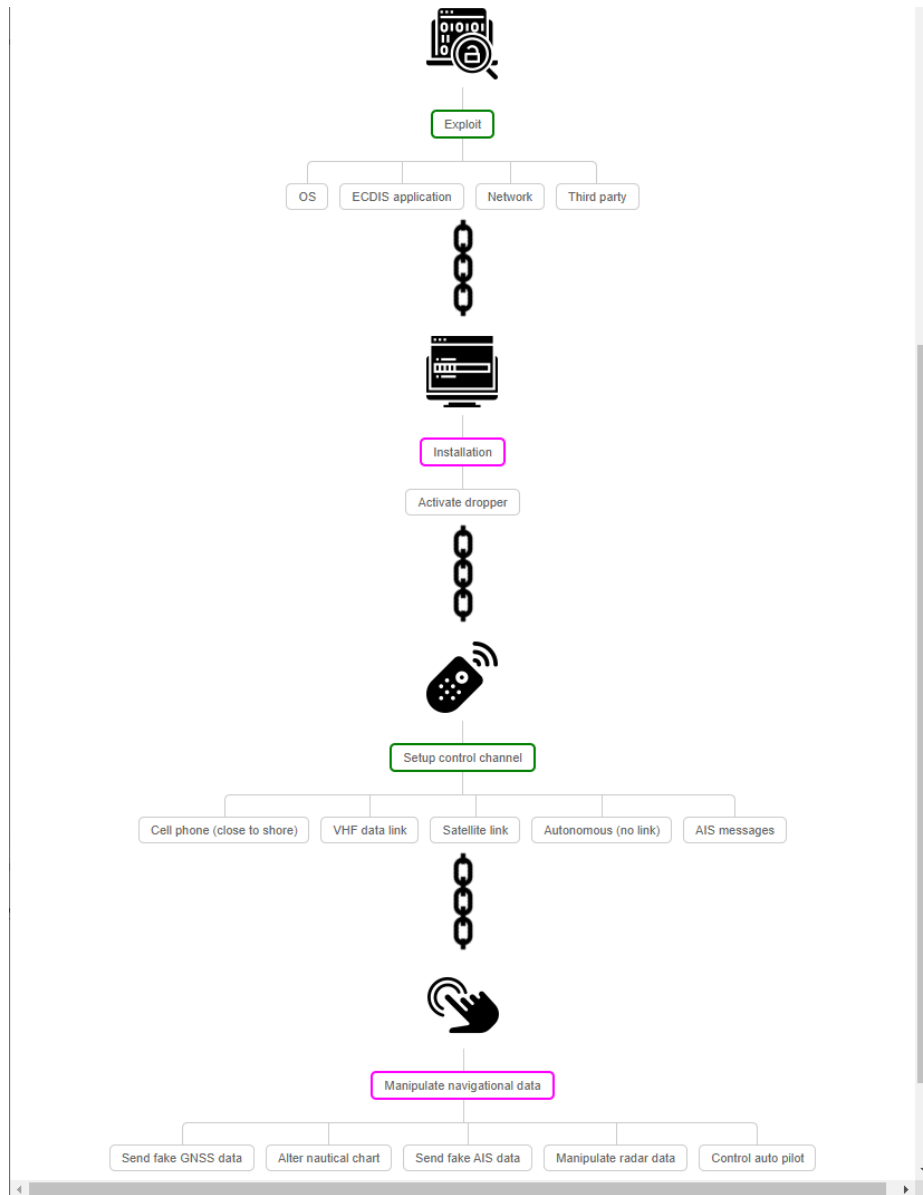






Fig.5: A screenshot from the last four stages; *Exploitation, Installation, Command and Control and Actions on Objectives*


B Cybercriminal profiles


 **Script kiddie (SK)** has a low level of motivation, thus *time consuming* attacks are not attractive to this profile. The technical skills are limited to *minimal* and the profile only accepts a *minimal* cost. Script kiddies will only utilize resources that can be realized *legally* and have *external* access.


 **Hactivist (H)** has a medium to high level of motivation anchored in the political cause they represent, thus they may conduct *time consuming*, targeted attacks. The technical skills of a hactivist is limited to *minimal*. In order to fight for their cause, the hactivist accepts *some* expenses. The hactivist is willing to require resources *illegally* and have *external* access level.


 **Vandal (V)** has a low to medium motivation and will only invest a *limited* amount of time in attention seeking attacks. The technical skills of the vandal is limited to *minimal* and the profile accepts a *low* cost. Vandals will only utilize resources that can be realized *legally* and have *external* access.


 **Petty criminal (PC)** has a medium motivation level, willing to invest *some* time in attacks that bring financial gain. They possess *operational* technical skills and accepts a *medium* cost. The petty criminal is willing to require resources *illegally* and has *external* access level.

 **Mobster (M)** has a medium to high level of motivation given that financial gain is possible, thus they may conduct *time consuming* attacks. The technical skills are *operational* and the profile accepts *costly* attacks. Mobsters won't second guess *illegal* resources and have *external* access level.

 **Cyberwarrior (CW)** is a state-sponsored actor with a high motivation level, thus will conduct persistent, *highly time consuming* attacks. The cyberwarrior has *adept* technical skills for launching any attack. In addition, the cyberwarrior is *not limited* by any costs and disposes resources that may be required *illegally*. As an immediate result of the *adept* skill level, the cyberwarrior has *internal* access.

 **Terrorist (T)** tends to be highly motivated and well funded, thus can conduct *time consuming* and *costly* cyberattacks to front beliefs. The technical skills are limited to *minimal*. The Terrorist is willing to require resources *illegally* and have *external* access level.

 **Internal - Hostile (IN-H)** has a medium motivation level and may launch attacks that require *some* time. The profile knows the system well, which yields an *operational* technical skill. *Some* expenses are acceptable, limited to *legally* acquired resources. Internals have *internal* access level by default.

 **Internal - Non-hostile (IN-NH)** launches cyberattacks by accident, thus *not* motivated at all to invest any time or money in a cyberattack and will only possess resources that can be *legally* realized. Given that accidental cyberattacks are possible yields an *operational* skill level and an *internal* access level.