Disruptive Advanced Persistent Threats in Critical Infrastructure, modelling and application in incident reporting

Meijaard, Yoram J.

Award date:
2020

Disruptive Advanced Persistent Threats in Critical Infrastructure, modelling and application in incident reporting

1st Yoram Meijaard
Eindhoven University of Technology, TNO
Eindhoven, The Netherlands
y.j.meijaard@student.tue.nl
yoram.meijaard@tno.nl

Abstract—**Disruptive Advanced Persistent Threats (D-APTs) are a new sophisticated class of cyberattacks targeting critical infrastructures. Whereas regular APTs are well-described in the literature, no existing APT kill chain model incorporates the disruptive actions of D-APTs and can be used to represent D-APTs in data. To this aim, the contribution of this paper is twofold: first, we review the evolution of existing APT kill chain models. Second, we present a novel D-APT model based on existing ATP models and military theory. The model describes the strategic objective setting, the operational kill chain and the tactics of the attacker, as well as the defender's critical infrastructure, processes and societal function. To showcase the model, it is applied to the BlackEnergy3 cyberattack.**

APT research is limited by the minimal availability of primary source data. To mitigate this data availability problem, we propose an application of the model in reporting of critical infrastructure incidents. Specifically, we provide a structured format to exchange critical infrastructure incident data using an industry standard.

Index Terms—**Advanced Persistent Threat, Critical infrastructure, Data Model, Cyber Situational Awareness**

I. Introduction

Cyberattacks span a range of attack techniques, levels of sophistication and stealthiness. In the upper-echelons of cyberspace we find Advanced Persistent Threats (APTs), highly sophisticated cyberattacks potentially posing a significant threat to national security [1]. Traditionally, APTs focus mainly on espionage. In recent years they have shown to be capable of disrupting important infrastructures such as the power grid [2] and nuclear facilities [3]. Changing the objective from stealthy extraction of information to disruption of ongoing processes distinguishes a new class of Disruptive APT (D-APT) attacks: sophisticated cyberattacks aimed at disrupting the normal operation of critical infrastructures.

Critical infrastructures (CI) support the critical processes (CP) of a nation. A prominent example is the power grid infrastructure which supports the process of supplying electricity to households and industry [4]. CPs are essential for the maintenance of critical societal functions [5]. Attacks on a CI may disrupt the corresponding CP, potentially leading to enormous socio-economic consequences. When one CP depends on the outcome of another CP, this is denoted as a dependency [5]. When such dependencies exist, there is a potential for cascade effects where the disruption of one CP causes the disruption of one or more other CPs [6].

This paper addresses two open problems. Firstly, while regular APTs are well-described in the literature, no existing APT model incorporates the disruptive actions of D-APTs and can be used to represent D-APTs in data. Secondly, limited data is available to researchers who wish to perform quantitative research about real world incidents. We discuss these problems subsequently.

While D-APTs are a relatively novel phenomenon, general APT attacks have existed for some time and have been researched intensively by both industry and academia. An important discovery is that APTs typically adopt a *kill chain*: a sequence of steps to obtain a certain goal [7]. Kill chains are used to describe APT attacks and have gradually evolved. In this paper, we review the evolution of cyber kill chains, show how these are currently not capable of describing D-APTs in sufficient detail and present a novel kill chain designed specifically for D-APTs.

As the goal of most APTs is espionage, which is typically attributed to intelligence agencies, it is no surprise that little is known about the attacker's operations. However, the goal of most D-APTs is disruption and sabotage, which is more commonly associated with military operations. Therefore, we turn our attention towards public military theory and doctrine to understand the operation of D-APTs. Armed with these, this paper proposes a model for D-APTs centred around the newly designed kill chain.

A thorough understanding of CI is required to fully understand the effects of a D-APT. This requires a comprehensive model that describes the CI from its technical infrastructure, up to the role it plays in society. By combining existing models, this paper proposes a comprehensive CI model which forms a suitable counterpart to the proposed D-APT model.

With respect to the limited availability of data, it should be noted that research about real world incidents can often only rely on reports published by industry [1]. This brings two major concerns: 1) *consistency:* reports present incidents in an unstructured or incompatible manner, typically using free-form textual discussions following their own models which are incompatible with reports about the same incident but from other vendors; 2) *monopoly:* vendor reports suffer from (implicit) biases and incentives including focussing on the highly sophisticated APT groups, leaving less sophisticated groups with little scrutiny [1]. These reports cannot present the full picture of APT attacks. The dichotomy of APT research is that despite these drawbacks, the desolation of data sources necessitates the usage of industry reports.

This paper cannot present a solution to the data availability problem. However, we can make a small step forwards. The proposed D-APT and CI models can be used to derive a structured data-model that can be used in incident reporting. Incident reporting is concerned with presenting the complete picture of what *has* occurred during an incident. Sharing and storing structured incident reports might make more data available to facilitate the empirical study of APTs.

More specifically, the main contributions of this paper are:

- an evaluation of the evolution of APT kill chains, revealing the gap between current kill chain models and the specificities of D-APTs;
- a novel kill chain and organisational model for D-APTs based on military theory and doctrine, describing the D-APTs tactics, operations and strategy;
- an integrated CI model which relates the technical operations, processes and societal functions of a CI;
- an architecture for D-APT incident reporting including a novel database schema and (semi-)automated data collection using industry standards.

The remainder of this paper is structured as follows. The next section discusses the used methodology. Section III introduces the literature regarding CI, cyberattack taxonomies and military theory. Section IV presents a review of the evolution of APT kill chains, elaborates on the designed D-APT and CI models, and showcases the models. The incident reporting architecture is provided in Section V. Section VI discusses the derived models and limitations of the approach. Finally, Section VII concludes the paper and provides directions for future work.

II. Methodology

The methodology used in this paper is three-pronged: conduct a literature review to collect all relevant theory, iteratively derive the models from the obtained theory and qualitatively evaluate that model against a suitable use case. This methodology is consistent with previous academic endeavours [8] [9].

More specifically, the literature study has two parts: 1) a literature review regarding APT models and cyberattack taxonomies, and 2) a literature overview regarding CI models, CI incidents and military theory. The goal of the review is to find most, if not all, existent APT kill chains and models. To do so, we conduct a structured backwards/forwards search through academic literature, combined with systematically searching the university library using keywords, until additional efforts no longer yield new material. The keywords are derived from articles retrieved in the search process and include: *advanced persistent threat* and *offensive cyber operations* in conjunction with *model*, *process*, *taxonomy*, *operations* or *strategy*. The shorter literature overview only follows keywords and a limited set of suggested documents.

The construction of the models is done iteratively. The models for D-APTs and CI are constructed independently, taking into account the identified relevant literature. They are both validated using a representative real world use case. Finally, the designed database schema and incident reporting model were directly derived from the proposed CI and D-APT models.

III. Literature overview

This section begins with a discussion about CIs and their characteristics. Section III-B discusses existing cyberattack taxonomies, which places APTs in perspective to other cyberattacks. Section III-C discusses APTs and their differences to D-APTs. Finally, Section III-D concludes by discussing relevant military theory and doctrine.

A. Critical infrastructure

Critical infrastructures are large technological systems of, typically unintentionally, increasingly intertwined independent elements [10]. These systems can be mapped onto a spectrum of criticality, ranging from *non-critical*, to *critical*, to *devolving criticality* i.e. a system on which mitigation measures are taken to reduce its criticality [10]. The impact of disruption of a CI depends on its criticality level, the breadth of the disruption and the related cascade effects [10]. The cascade effects can be described in terms of severity, ranging from little effect on other systems, to completely bringing down other systems [10].

Cascade effects can only occur if there exists a CI dependency i.e. the output of one CI is required for the operations of another CI. An interdependency is a mutual dependency [5]. These (inter)dependencies can be characterised as a physical, cyber, geographic or logical interdependency [11]. Two other effects that can occur when a CI dependency exists are escalating effects, where a failure in one CI increases an existing failure in another CI, and common cause failures, where two CIs are disrupted due to a common cause [11].

Cascade effects are reasonably common [6]. In an empirical investigation of 830 CI incidents reported in publicly available news media, evidence was found for frequent patterns of sequential failures called pathways [6]. In particular, the energy sector is a common initiator of such a pathway. These pathways are the dominant route of cascading failures, although exceptions exist. Contrary to common single cascades, multiple subsequent cascades, although theoretically possible, seem to occur rarely in practise.

Many taxonomies have been proposed for CI disruption threats. An early attempt by Luijf et al. was an extensive framework for classifying these threats [5]. Crucially, the taxonomy by Luijf et al. classifies APTs solely as a software related threat, which ignores the insider threat and human element of APTs [12] [3]. A more recent taxonomy discusses current technological trends and their related security issues, in particular the increased exposure of CI to the internet [13]. More concrete examples of common CI vulnerabilities include legacy software, insufficient isolation and default passwords [14]. Finally, a recent policy document of the Dutch National Coordinator anti-Terrorism and Security highlights that attacks occur in a hyperconnected infrastructure, which complicates determining the attack origin [4]. They note that crisis organisations responding to an attack depend on CI and that there is a large involvement of private entities in managing CI, both of which are a potential weakness.

B. Cyberattack taxonomies

Cyberattack taxonomies establish the landscape of cyberattacks in which to contextualise D-APTs. Howard et al. [15] propose an early cyberattack taxonomy which distinguishes attacks based on the argument that attacks consists of attackers, using tools to exploit a vulnerability, which constitutes in an action on a target, resulting in an unauthorised result obtaining an objective. Hansman and Hunt [16] argue that any list or tree-structured taxonomy is not applicable to attacks with characteristics of multiple categories. They propose that a taxonomy should consider all attack characteristics independently as granular dimensions. The taxonomy by Howard et al., as well as the taxonomy by Hansman and Hunt, focus on the technical capabilities of cyberattacks. A different approach is proposed by the cyberthreat taxonomy AVOIDIT, which emphasises the attack impact [9]. AVOIDIT uses data tuples describing an attack vector with operational impact evading defence and causing information impact in a target. In AVOIDIT, operational impact refers to the mechanism of the cyberattack (e.g. malware, virus, etc.), while information impact is the effect caused by the mechanism. Furthermore, Uma and Padmavathi propose a taxonomy of the purpose, legal status involvement of the attacker and the scope of the attack [17].

Although extensive, none of these taxonomies include APTs. The taxonomy proposed by Bahrami et al. classifies the phases of APT attacks based on a commonly used kill chain [8]. This taxonomy is “living”, that is, the taxonomy is extended as APTs evolve, ergo D-APTs can be included. The Actor Lever, Effects and Response Taxonomy (ALERT) combines the technical, motivational and impact side of cyberattacks and is applicable to APTs [18]. Actors are characterised based on their role, motivation, unit e.g. individual or group, plausible deniability e.g. state sponsored or not, and their reach. Levers represent the tactics of the attackers, which causes an effect. The response is the subsequent action taken by the defender.

C. Advanced persistent threats

APTs are highly sophisticated cyberattacks with large capabilities and resources. To illustrate, APTs typically require in-depth technological knowledge which necessitate a team of domain experts, programmers and security experts [3]. APTs are tailored to their target using substantial insider knowledge [3]. APTs are capable of developing and acquiring zero-day exploits [1], although their use is uncommon [19]. APTs can replace their exploits between attacks, but are known to reuse their infrastructure [7] [19] [20]. Another upcoming practice is living off the land, where the attacker abuses already installed system tools rather than exploits [19]. APTs try to evade detection, for example by attacking the operator’s response capacity [3].

Despite the significant capabilities of APTs, there are recommended defensive strategies. Technical strategies include defence in depth, patch management, strong network access control, monitoring, and the use of honeypots [3] [21]. To combat the insider threat of APTs, a multidisciplinary approach is suggested focussing on deterrence, for example by creating an environment that discourages insiders turning against the organisation [12]. However, in practise only a subset of such protective measures are in place, even in sensitive environments [3].

Research on APTs typically relies on technical reports produced by the large security vendors [8]. To help find the right information, Lemay at al. analysed and provided an overview of 40 different APT groups [1]. A problem with limited available data is a bias against less technically sophisticated APT groups, as the security vendors gravitate towards the advanced groups [1]. Despite the limited availability of data, Lemay et al. identified a few knowledge gaps regarding APTs [1]: 1) there is a gap between technical and operational knowledge, that is, what malware is used in an attack is known, but how the attack is structured and organised is less clear; 2) the role of reconnaissance and support in APT is currently unclear, which includes the process of target selection. Note that both gaps in literature are addressed in the model proposed in Section IV.

Disruptive APTs (D-APTs) are a subset of regular APTs and have similar characteristics. D-APTs are highly sophisticated attacks with large capabilities and resources, directed at a specific target. D-APTs follow a kill chain and involve similar tactics to APTs, such as zero-day exploits and living off the land. The primary difference between APTs and D-APTs is in their purpose. APTs are espionage-oriented, their goal is to extort information from an organisation. On the other hand, D-APTs are sabotage-oriented, their goal is to disrupt critical infrastructure. Consequently, there are several other differences between APTs and D-APTs, an overview of which is given in Table I.

D-APTs are cyber-physical attacks, because Operational Technology (OT) such as critical infrastructure are cyber-physical systems. Disruption of the critical infrastructure requires extensive domain knowledge, for example to find the vulnerable components of the system. Note that vulnerable is not merely limited to the software, but includes the hardware of the disrupted component. The hardware must be essential to the operation of the system to disrupt the system. These cyber-physical components are not trivial to acquire and might require substantial resources.

D-APTs will always have a noticeable effect. Consequently,

TABLE I
COMPARISON APT AND D-APT

Characteristics	APT	D-APT
Targetted	Yes	Yes
Highly sophisticated	Yes	Yes
Goal	Espionage	Disruption
Cyber-physical	No	Yes
Required resources	IT	IT + OT
Effect duration	Years	Months
Rehearsal	Yes	Difficult

an operator of a critical infrastructure will discover that *something* is wrong and investigate accordingly. A normal APT attack can be active in a network for years to gather and exfiltrate information [1]. This is not applicable to D-APTs, as the attack will be discovered when the disruption occurs.

As the disruption will be discovered the attack needs to be well-executed in order to be effective. Preparation is therefore crucial. The attacker must select a suitable target, which requires extensive reconnaissance. The attack must be well-rehearsed, despite the difficult acquisition of the involved hardware-components. Rehearsal of normal APT is less complicated, as it does not involve acquisition of these hardware-components.

D. Military theory and doctrine

The military is turning their attention towards the cyber domain, enabling researchers to study disruptive cyberattacks though the published military doctrine. In this paper, we will primarily discuss the doctrine published by the U.S. Department of Defense (DoD). This section follows the three levels of cyberwarfare, that is, the strategic, operational and tactical level [22].

The **strategic level** concerns objective setting and planning operations to achieve these objectives. The strategy is about deciding what operations need to be conducted, which in practise will be multiple operations conducted in parallel [23]. To achieve their objective, the operations need to satisfy a set of functions inherent to all military operations [23]. Specifically, each operation requires *command and control* to direct the attack, the gathering of *intelligence* about the target and the development of appropriate *firing* capability. The attacker must be able to *move and manoeuvre* to execute the operation and must *protect* against counter-actions. After the operation, lessons learned need to be dispersed for *sustainment* of the organisation. Next to these functions, there are specific strategic considerations for cyber operation planning [23]. The attackers require an overview of the (higher order) effects of the operation, although this is difficult to predict. Similar to CI incidents, the higher order effects can be cascading, compounding or collateral. Another consideration is the *reversibility* of an attack. If an attack is irreversible and backfires, then this might be catastrophic. In planning the operations, *timeliness* is important to prevent operational deadlocks. Finally, as cyberspace is complex and dynamic, the operation needs to be *flexible*.

The **operational level** concerns the execution of the attack. An important operational concept is Situational Awareness (SA), which addresses the perception of the environment [24]. More precisely, SA is described as a state of knowledge about the operating environment and comes in three levels:

1) Perception: knowing what elements are in the environment
2) Comprehension: knowing how these elements interact with each other
3) Projection: knowing how to manipulate the elements to achieve a goal.

SA is required to effectively manipulate the environment, as even a competent operator will make mistakes if their SA is wrong. The capacity to obtain SA depends on the actor's experience. For example, when exploiting a system an experienced hacker will have a higher state of SA then a rookie. Because short term memory is limited, SA cannot be sustainably retained through perception only. For example, in a security operating centre too much information is received to perceive, but by comprehending the alerts the operator still has high SA. The theory of SA is typically applied in situations where many decisions need to be made in a short period. SA in the cyber domain typically constitutes network operators using automated techniques to perceive their network [25]. Less commonly, SA is applied in a situation where there is too little information to obtain high levels of SA. However, Ahmad et al. use SA in the design of their APT kill chain [26]. They argue that disrupting the attacker's SA disrupts the entire APT, for example by mixing real data with fake/offensive data.

Using the theory of SA, the DoD describe a six phase targeting cycle [27]. First the *end state* is determined and the potential targets are *prioritised*, which requires sufficient SA regarding the targets. Once a suitable target is selected, the attacker analyses his own *capabilities* and picks an appropriate action for engagement. After *approval* the attacker *executes* the attack and concludes by a *reflection*. The actual execution of the attack follows the F2T2EA kill chain [27] [28]. F2T2EA is an initialism and describes a kill chain. In F2T2EA an actor continuously scans for targets until they *find* a target. They *fix* on one target in particular and *track* the target until a suitable opportunity presents itself to attack. At which point they *target* their weapons and *engage*. Afterwards there is an *assessment* phase in which the attack is evaluated.

Another operational model is the Terrorist Life Cycle (TLC) [29]. The goal of the TLC is to guarantee selecting successful targets by emphasising reconnaissance. The TLC starts with *broad target selection*, roughly deciding which target to attack, the potential target is put under *surveillance* and when enough intelligence is gathered then a specific target is *selected*. This selection process builds up SA and very carefully selects a target. At this point, the attack is *rehearsed* to eliminate mistakes. The attack is *executed*, after which the terrorists will *escape* from the scene. The rehearsal step is unique to the TLC.

The **tactical level** of warfare includes the OODA decision process designed by Boyd [30]. OODA is an initialism for

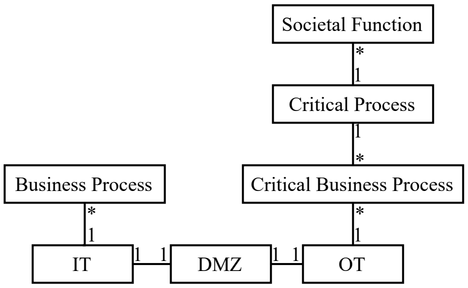

Fig. 1. Overview of all entities in the CI model, where each line indicates a cardinality relation e.g. one CP can execute multiple functions.

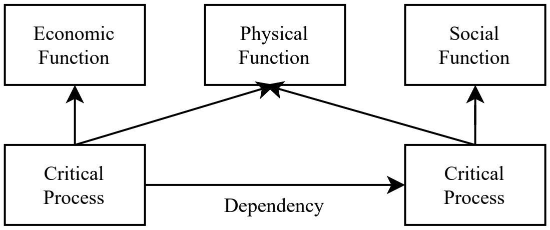

Fig. 2. Societal level of the CI model. Critical processes fulfil societal functions and depend on other critical processes.

Observe, Orient, Decide and Act. The OODA-loop consists of perceiving new information about the environment, orienting yourself in the perceived environment using previous experience, deciding what tactic to use next and acting that out. The action affects the environment, creating new perceptions, etc. Boyd's thesis states that the actor with the quickest execution of the OODA-loop will always come out on top.

IV. Modelling CI and APTs

This section begins with a description of the critical infrastructures (CI) model. In Section IV-B the evolution of APT kill chains is evaluated and motivated why neither of them is suited to describe D-APTs. In Section IV-C the D-APT model is described. Note that the CI model describes *what* is attacked and the D-APT model describes *how* it is attacked. Finally, the proposed models are evaluated in Section IV-D.

A. CI model

The core of the CI model is that a critical infrastructure (CI) supports a critical process (CP) which fulfils a societal function. The CI model has three levels: *technical*, *process* and *societal*. At the technical level, there is an infrastructure consisting of Information Technology (IT) and Operational Technology (OT), separated by a Demilitarised Zone (DMZ). Within an organisation, the IT systems support one or more business processes (BP), while the OT systems support one or more critical business processes (CBP). These processes come together at the process level to form a critical process (CP). At the societal level, the CP performs one or more functions that are so crucial for society that the process is labelled critical [4]. An overview of these relations is given in Figure 1.

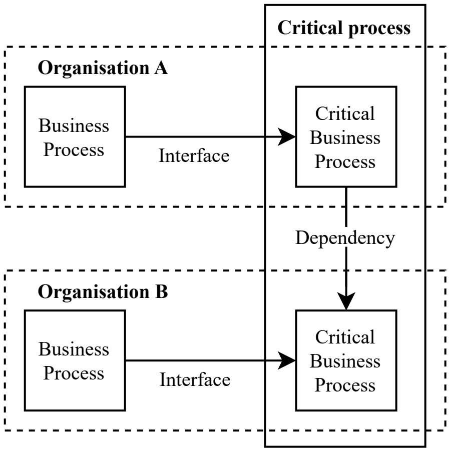

Fig. 3. Process level of the CI model. Critical processes consist of interconnected critical business processes executed by different organisations. The regular business processes within an organisation can affect the critical business process, this mechanism is called an interface.

1) Societal level: The societal level concerns the effects of CPs on society, which is summarised in Figure 2. A process is critical if it fulfils one or more societal functions of the type:

- *economic*: the CP is crucial for the economy, or
- *physical*: the CP physically protects society, or
- *social*: the CP is crucial for the social order [4].

If a CP depends on another CP, then a cascade effect can occur. The effect of such cascade is a disruption of the societal functions. Therefore, the dependencies are modelled on the societal level, even though they are not societal functions. This level is modelled after the definitions by the NCTV [4], but focusses on the function of the CPs rather than the impact of a disruption.

2) Process level: The process level describes the organisation of a single CP, which is summarised in Figure 3. A CP is a complex structure of multiple CBPs depend on each other to work towards the same goal. The dependencies are expressed with a directed graph where $CPB_A \rightarrow CPB_B$ indicates that B is dependent on A. This is a generalisation of the linear model proposed in [31], which allows the expression of more complex CPs. The organisations responsible for CBPs have additional non-critical BPs which can influence a CBP. This interface is where disruption of a BP influences or even disrupts a CBP and is modelled through the same directed graph.

3) Technical level: The technical level describes a single organisation and their infrastructure, which is summarised in Figure 4. The technical level is a simplification of the Purdue Reference Architecture [32] and consists of three distinct areas: an IT network, an OT network and a DMZ in between. The IT network performs BPs, such as email, hence requires an internet connection. The OT network performs CBPs, which in principle can be executed with little outside connection. The goal of the DMZ is to ensure that threats from the IT network cannot reach the OT network. In practise there are

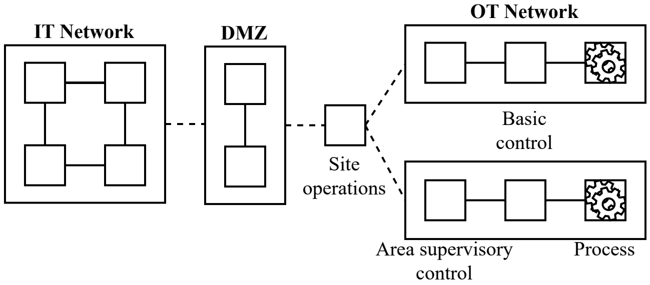

Fig. 4. Technical level of the CI model based on the Purdue Reference Architecture [32]. IT and OT are separated by a Demilitarised Zone. In the OT network there is central control at *site operations* and local stations, each with their own local control at the *area supervisory control*.

processes that occur in the DMZ, such as patch management, which possibly allow the attacker to pivot through the DMZ.

B. Evolution of APTs

Numerous APT models have been proposed over time, each improving upon the models before. This evolution is caused by an increased understanding of APT attacks and the evolution of the attacks themselves. This section provides an overview of the evolution of APT models and kill chains by discussing each model briefly and relating the model to its predecessors. An overview of the evolution of APT models is given in Figure 5. In general, this section discusses two categories of APT models: 1) Process models, which are concerned with a higher level operational view of APTs. Process models are discussed in Section IV-B1. 2) Technique, Tactics and Procedures (TTP) models, which are unordered lists of the TTPs used in an APT. Compared to process models, these are lower level models discussing the details of an APT with less emphasis on the overall structure. TTP models are discussed in Section IV-B2. In Figure 6 an overview of all discussed APT models is given.

1) Process models: The common model for APTs is the Cyber Kill Chain (CKC) by Hutchins et al. [7], which is an adaptation of the F2T2EA kill chain [28] discussed in Section III-D. The adaptation is thusly: the find, fix and track phases are merged into reconnaissance, targeting became weaponization and engagement is expanded into the remaining phases of the CKC. The CKC is a linear model, hence a single CKC might be insufficient to describe every APT [7]. Another criticism is that the CKC hides many steps in its final phase, as *actions on objectives* is quite indistinct.

Several authors have proposed improvements to the CKC. Chen et al. combine the CKC phases *exploitation* and *installation* into *initial intrusion* [21], add *lateral movement* and specify *action on objectives* as *data exfiltration*. Similar to Chen et al., Bryant and Saiedian include *lateral movement* and *data exfiltration*, and add *privilege escalation* [33]. Malone proposes a three-part Extended Cyber Kill Chain (ECKC) [34] consisting of: 1) the "legacy" CKC to breaks the perimeter of the network; 2) an Internal Kill Chain to move laterally and obtaining access to the target; 3) a Target Manipulation Kill Chain to achieve the desired goal. These three parts address the occasional inability of a single CKC to describe an APT and the Target Manipulation Kill Chain addresses the indistinct final phase of the CKC. Malone notes that an attacker can take several parallel actions in a phase, out of which one succeeds, and notes that this is "tree-like" behaviour instead of linear. Finally, Malone indicates that it takes months to execute the ECKC.

Another category of models feature circular behaviour, that is, where the attacker might go through a phase more than once. A first attempt was the Attack Lifecycle Model (ALM) by Mandiant [35]. The ALM contains an external and internal part. The external part is linear and its three phases are effectively a condensation of the CKC. The internal part consists of iteratively executing reconnaissance, moving laterally, maintaining presence and taking actions. As the internal part is executed iteratively, the ALM emphasises short intertwined actions rather than the extensive single phases of the CKC.

Rutherford and White propose that the internal phases are not sequential but bidirectional, where the attacker can go back and forth between phases [36]. Similar to Chen et al. they include the extraction of information as the final phase. Kim et al. add iterative behaviour to the CKC to describe that the attacker might execute the CKC multiple times in a row to achieve their goal. Additionally, they include an iterative internal kill chain, as APTs have characteristics of insider threats [37]. Note that the internal chain is equivalent to the first five phases of the CKC.

Ussath et al. proposed a model that simplified the CKC to only three dimensions [19]. Each dimension corresponds to the actions the attacker can take that would be *detectable* by the defenders. Thonnard et al. propose a model for the general category of targeted attacks, therefore it is less detailed [20].

Ahmad et al. propose the APT Operational Line (APTOL), which is similar to the CKC but uses terminology drawn from military doctrine [26]. Compared to the CKC, the APTOL places more emphasis on vulnerability assessment, sustaining access and lateral movement.

All previous models are focussed on *general* APTs and lack CI specific elements. The kill chain that comes closest to describing a D-APT is the two stage Industrial Control Systems Cyber Kill Chain (ICKC) proposed by Assante et al., which consists of the regular CKC, followed by a second stage of developing, testing and executing ICS specific malware [38]. A critique is that this kill chain does not describe how the attacker got to the ICS systems, nor does it explain the purpose of the developed malware.

2) TTP models: Tactics, Techniques and Procedures are respectively the goal, means and implementation of an attack. Detailed TTP models describe per tactic what the procedures are. However, in this paper we focus solely on the tactics.

A commonly used TTP model is the MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) framework [39], which describes, in no particular order, APT tactics based on empirical evidence. The Enterprise

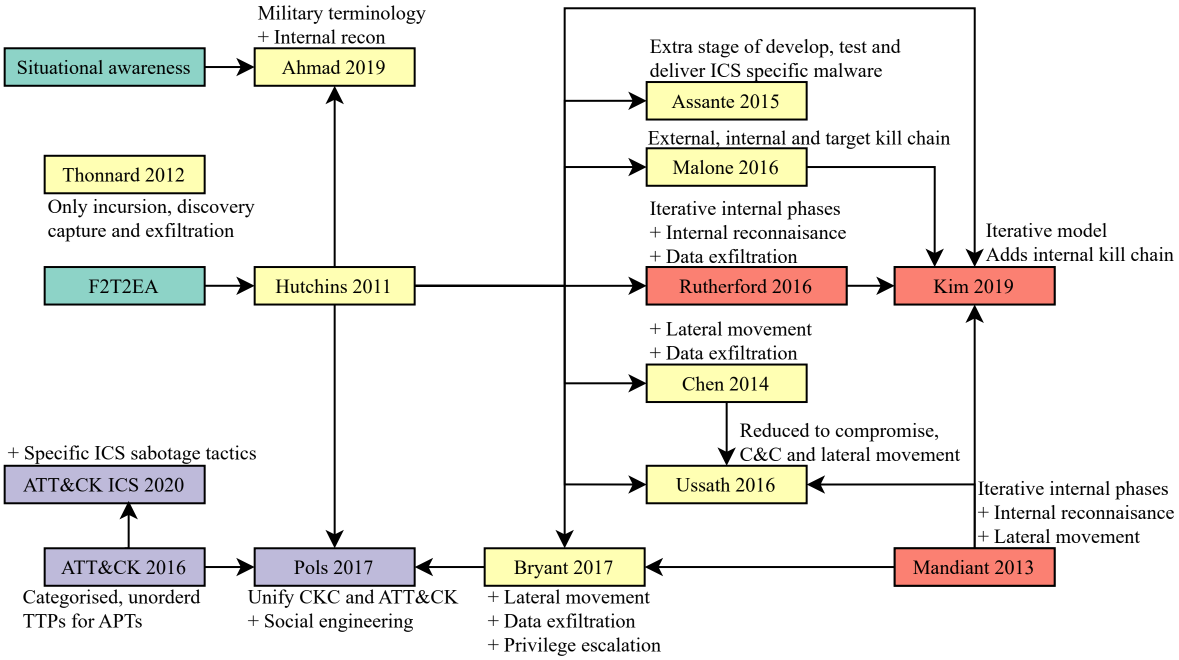

Fig. 5. Overview of the evolution of all APT models described in Section IV-B. Each arrow $A \rightarrow B$ indicates that A influenced B.

variety of ATT&CK emphasises exfiltration of data, while the ICS variant emphasises disruptive operations such as *Inhabit Response Function* and *Impair Process Control*.

Pols proposes the Unified Kill Chain (UKC) [40], which is an extensive list of TTPs unifying the CKC by Hutchins et al. [7] and ATT&CK Enterprise [39]. Additionally, the UKC includes *social engineering* and *target manipulation* as specific tactics. Social engineering is referred to as a technique in ATT&CK and target manipulation is borrowed from the Expanded Kill Chain by Malone [34].

3) Discussion: Based on the differences between APTs and D-APTs, as described in Section III-C, we can derive a set of criteria to evaluate the suitability of these existing models to describe D-APTs. An overview of this evaluation is given in Table II.

The first criteria is that the model must describe disruptive actions. Only the models by Assante et al. and ATT&CK ICS describe this explicitly. The common final phase in the existing models is *action on objectives*, which could implicitly describe disruptive actions. Other models include a (variant of a) data exfiltration phase, which highlights that the model is designed for espionage-oriented APTs.

The second criteria is that the model must describe the attackers movement through the network. In D-APTs the attacker must find their way to the OT network, which is located far from the initial intrusion. Tangentially, an D-APT will always require pivoting through the protections surrounding the OT network, which is only included in the model proposed by Pols.

Finally, the model must describe an extensive preparation phase. Almost all models include reconnaissance and most include weaponization. However, preparation for D-APTs is more extensive and includes selection of an appropriate target and rehearsing the attack. Target selection and attack rehearsal are the third and fourth criterium respectively.

TABLE II
COMPARISON SUITABILITY OF EXISTING APT MODELS TO DESCRIBE D-APTS

	Disruption	Movement	Target selection	Rehearsal
Hutchins et al.	Implicit	-	-	-
Mandiant	Implicit	Yes	-	-
Chen et al.	-	Yes	-	-
Bryant	Implicit	Yes	-	-
Ahmad et al.	Implicit	Yes	Yes	-
Rutherford and White	Implicit	-	-	-
Kim et al.	Implicit	-	-	-
Malone	Implicit	Yes	-	-
Assante et al.	Explicit	-	-	Yes
Thonnard et al.	-	-	-	-
Ussath et al.	-	Yes	-	-
ATT&CK Enterprise	-	Yes	-	-
ATT&CK ICS	Explicit	Yes	-	-
Pols	Implicit	Yes	-	-

C. D-APT model

The D-APT model is divided into three levels and three dimensions. The levels are *strategic*, *operational* and *tactical* [22]. The dimensions are *attack structure*, *support artefacts*, and *mental model*. The attack structure are concepts related to the execution of the attack, such as a kill chain. The support artefacts are (non-material) artefacts that support the attack. The mental model captures the (perceived) mental state of the attacker. An overview of the D-APT model is provided in Table III.

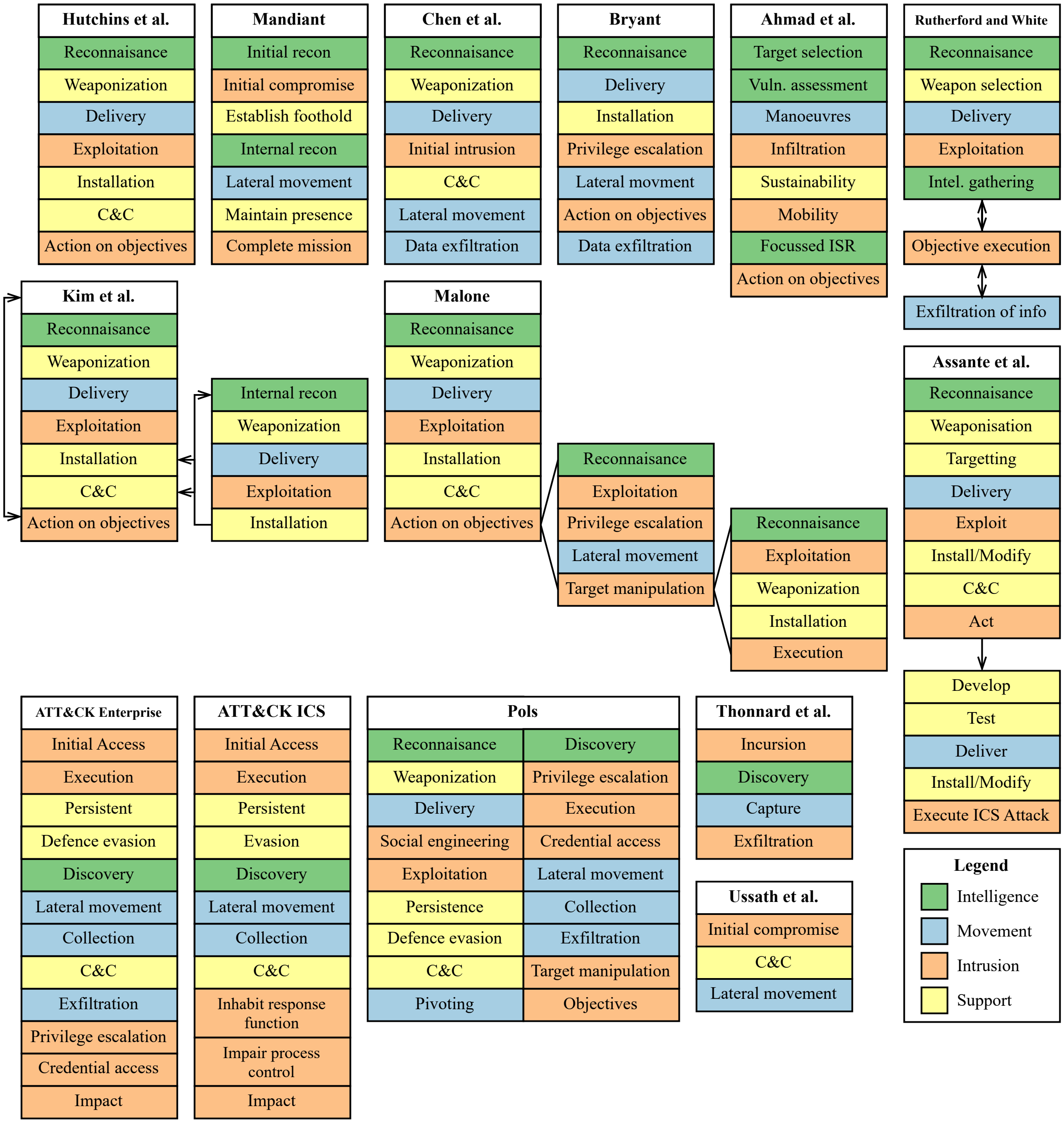

Fig. 6. Overview of all APT models in described in Section IV-B.

TABLE III
APT MODEL OVERVIEW

Level	Attack structure	Support artefacts	Mental model
Strategic	Objective setting	Organisation	Motivation
Operational	Kill chain	Infrastructure	SA
Tactical	TTPs	Tools	OODA

The first dimension is the attack structure, which consists of *setting objectives* that are achieved by a *kill chain* that use *TTPs*. There are many-to-many relations between these concepts, for example a single kill chain might satisfy multiple goals, and a goal is achieved by multiple kill chains. The support artefact dimension consists of an *organisation* that maintains an attack *infrastructure*, which in turn enables the use of *tools*. Artefacts enable the attack and can to a varying degree be reused [7] [19] [20]. The mental model dimension consists of the attacker's *motivation*, the *situational awareness* that is built up during the attack and the *OODA*-loop used in executing the attack.

At the strategic level, *organisations* are *setting objectives* driven by *motivation*. On the operational level, the *kill chain* uses *infrastructure* and successful execution depends on *sit-*

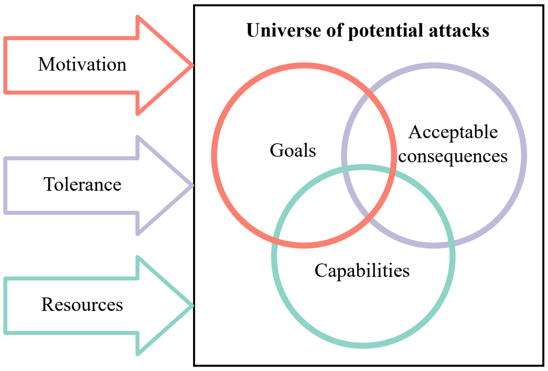

Fig. 7. Model depicting the strategic level of a D-APT attack. The rectangle depicts a universe of potential attacks. The three circles indicate restrictions which follow the factors indicated with an arrow.

uational awareness. Finally, on the tactical level, the *TTPs* are executed during the *OODA*-loop and require *tools* for successful execution. There is a correspondence between the levels of the D-APT model and the levels of the CI model. The strategic level objective setting determines which societal function is to be disrupted. The operational kill chain serves as the execution plan to disrupt the process level critical process. The tactical TTPs are the means with which the technical infrastructure is attacked.

1) Strategic level: The strategic level of a D-APT attack explains what factors are involved in strategically setting objectives for the attack, an overview of which is given in Figure 7. This level is modelled as a universe of potential attacks with three types of restrictions: *goals*, *capabilities* and *acceptable consequences*, which are influenced by three external factors: *motivation*, *resources* and *tolerance* respectively. There can be multiple restrictions of the same type. The restrictions' overlap identifies a set of viable attacks that satisfy the motivations of the attacker, can be executed with the available resources and whose consequences are tolerable.

The *motivation* of the attacker determines the desired *goals* of the attacker. For the purpose of this model a high level description of motivation, including which societal function is to be disrupted, suffices. The explanation of why the attacker has this motivation is not in the scope of this model, but note that motivation is not static and might change over time as the environment changes. Identification of the attacker's motivations provides intelligence as to the attacker's goals, hence gives insight into the expected attacks.

Resources are used by the organisation to create attack capabilities. The support structure organisation is crucial for the transformation of resources into capabilities. Advanced organisations have entire development divisions, tasked with acquiring, developing and maintaining the infrastructure and tools [41]. Furthermore, these organisations have operational divisions executing multiple parallel attacks, which require sophisticated coordination [41] [23]. Resources are not limited to finances, but include *human resources* who need to be recruited [41] [42]. In similar situations, disrupting the recruitment process is a way to combat the attackers [29].

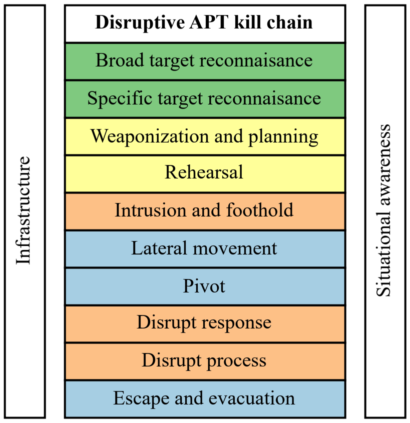

Fig. 8. Model depicting the operational level of a D-APT attack. The kill chain is supported by the artefact infrastructure and mental model of situational awareness. Note that the same colour scheme as in Figure 6.

The final restriction is *acceptable consequences*, that is, only attacks whose consequences are acceptable by the attacker should be executed. Whether the attacker finds a consequence acceptable depends on their *tolerance*. For example, some actors will not attack if there will be retaliation or if there will be collateral damage. Actors are aware of these consequences and take this into consideration when planning their operations [27] [23]. A larger tolerance implies a larger range of executable attacks. Some attacks can be slightly altered to mitigate the consequences, for example by excluding an entire country from being targeted thus not provoking them [43].

The strategic level ties together the attack and supporting processes, such as recruitment and development by including these in the resource factor. The result of the strategic level is a set of feasible attacks, targeting a societal function by disrupting the underlying critical process. Crucially, the identified attacks are within the resource capabilities of the attacker and the consequences of the attack can be tolerated.

2) Operational level: The operational level explains what kill chain is required to execute the attacks identified on the strategic level. This novel kill chain is created explicitly for APT attacks against CI and is summarised in Figure 8. Throughout the kill chain the support artefact *attack infrastructure* and the mental model *situational awareness (SA)* are discussed.

Broad target reconnaissance: investigate the potential attacks identified at the strategic level, which increases SA regarding the targets. Once sufficient SA is gathered, that is, the attacker is able to comprehend the attack space, then conclude by selecting a specific target.

Specific target reconnaissance: continue gathering SA regarding the selected target and concludes once the SA level of projection has been reached.

Weaponization and planning: prepares the attack by building or acquiring the tools required for the attack and coordinating this attack with the other potential attacks.

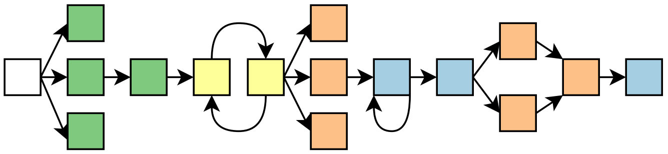

Fig. 9. An abstract example of a directed graph ordering of a D-APT. This example depicts multiple reconnaissance phases, going back and forth between planning and rehearsal. Intruding into the network after several failed attempts, moving laterally through the network, pivoting the DMZ. Disruption of the response and the process occurs simultaneously. Note that the same colour scheme as in Figure 6.

Rehearsal: executes the plan on a (representative) testing environment. Among others, this effectively validates that the SA projection level is reached. Rehearsal is possible for the disruption of a single CI, as a sufficiently resourced attacker can acquire enough hardware to create a realistic testing environment. If the attack should cause a cascade effect, then rehearsal is substantially more difficult. In practise CI operators are able to estimate risks of cascade effects [31], hence an attacker with an *extremely* thorough view of the architecture e.g. a senior level architect turned insider threat, could reasonably accurately predict such cascade effects. Prediction does not involve a testing environment, hence is not the same as rehearsal. This phase concludes either by advancing to the next phase as the testing was successful, or by going back to the drawing board.

Intrusion and foothold: penetrate the network and set up sufficient infrastructure to continue the attack. This phase concludes once sufficient infrastructure is setup, at a minimum it should allow the attacker access to the network without the need to penetrate it again.

Lateral movement: move through the network. This is particularly important for a D-APT as the target is typically located far from the computer initially penetrated. A particular tactic is “living off the land”, where the attacker abuses already existent system tools, which is virtually undetectable [44]. This phase concludes when a system is reached from which the attacker can move to the OT network, which requires that the attacker at least comprehends that they are in such a system.

Pivot: When two networks are separated by a single chokepoint system, the term pivot describes the attacker moving through that system [40]. In case of CI, the separation between IT and OT is achieved with a DMZ [32]. In this phase the attacker pivots through the DMZ, for which the attacker requires projection level SA regarding the DMZ. This phase concludes once the attacker gains access to the OT network.

Disrupt response: suppress the disruption response system of the CI, which naturally should occur before the disruption of the process. In a D-APT the desired disruption effect is naturally visible, by disrupting the response function the effects of the attacks are prolonged, for example by altering the operator’s dashboard [3] or by DDoS-ing the helpdesk [45]. The attacker requires a high level of comprehension of the system in order to ensure that *all* response functions are sufficiently suppressed, at which point this phase concludes.

Disrupt process: disrupt the critical process. Subtleness is key for D-APTs. An attack should execute the minimum disruption that accomplishes the goal to reduce the changes of the attack being detected. Executing the two disruption steps need not be done at the first opportunity. The attacker can reside in the network until a circumstance of increased efficiency occurs. For example, a D-APT targeting the emergency communication channels would have significantly higher impact when executed during a natural disaster.

Escape and evacuation: reduce the forensic footprint of the attack. For example by purging the hard drives of infected machines [45]. In order to remove all evidence, a high level of comprehension is required to enumerate *all* touched systems and potential evidence.

The kill chain’s purpose is to disrupt a CP. During *broad target reconnaissance* the attacker surveils the entire CP to choose its target CBP. The attacker must assess in what context this CBP is executed, that is, what role the CBP plays in the overall CP and that there are no redundant processes that could take over when the CPB is disrupted. During *specific target reconnaissance* the kill chain builds up enough SA for the attacker to disrupt the CPB. To successfully disrupt the response function, the attackers require intricate knowledge of the organisations processes to realise how the response function works and how it helps recover the CBP. Note that in general, the execution of the kill chain depends on the process level of the CI model, rather than the technical level.

The kill chain phases can be combined in different orders. As discussed in Section III, there are several options to combine phases: strict linear or circular orders, tree structures or no order. An argument can be made for each of these: a strict order is very specific and intuitive, while no order is very flexible. The counter argument is that flexibility provides little guidance and a strict order might be unsuitable for many attacks. A middle ground could be found in the tree ordering, however, these cannot express repetition. For the D-APT model a compromise was found by using a *directed graph* as its structure, with the presented order of the phases as a guidance. Directed graphs allow cycles, so repetition can be modelled. This is the most bare-bones structure that can reasonably be considered a structure, while allowing the greatest amount of flexibility. An example of a directed graph ordering of a D-APT is given in Figure 9.

The D-APT kill chain is based on several models given in Section III. The reconnaissance, planning and rehearsal phases were modelled after the TLC [29], which was chosen for its excellent reconnaissance description. The phases intrusion, lateral movement and pivoting are found in the models by Chen et al [21], Mandiant [35], Bryant and Saiedian [33], and Pols [40]. The disruption phases are a generalisation of the concepts introduced in ATTACK ICS [46]. Escape and evacuation are taken from the TLC [29]. Contrary to other models, intrusion and foothold are taken together as solely intruding into a network is useless without some structure to do it again with less effort. Finally, similar to Ahmad et al. [26] SA is used in the D-APT kill chain to provide an explanation

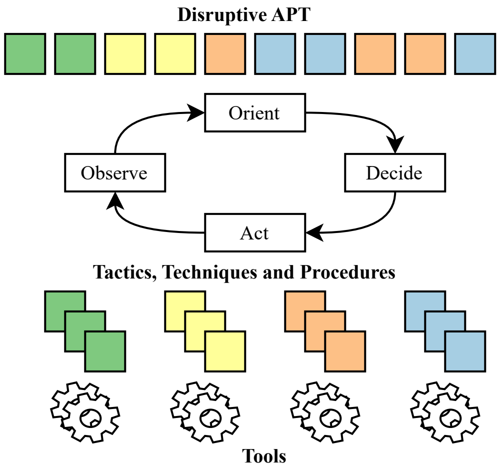

Fig. 10. Model depicting the tactical level of a D-APT attack. This model uses the OODA-loop to relate the kill chain to the corresponding TTPs. In turn, the TPPs are supported by tools. Note that the same colour scheme as in Figure 6.

TABLE IV
PHASES OF D-APT KILL CHAIN MAPPED TO TTPS (CATEGORIES). * TTP CATEGORY GIVEN IN ATT&CK ICS [46]. † TTPS BASED ON BAHRAMI ET AL. [8]. ‡ TTPS BASED ON THE DOD [27] [23].

D-APT Kill Chain	TTPs
Broad target reconnaissance	Discovery*, Collection*, Social engineering†
Specific target reconnaissance	Discovery*, Collection*, Social engineering†
Weaponization and planning	Define joint functions‡, Define end state‡, Capability assessment‡, Targeting‡, Obtain approval‡, Abusing vulnerabilities†, Subterfuge techniques†, Web equipping† Legitimate digital certification†
Rehearsal	Full replica testing, Partial replica testing, Emulated testing, Theoretical analysis
Intrusion and foothold	Command and control*, Execution*, Persistence*
Lateral movement	Lateral movement*
Pivot	Lateral movement*
Disrupt response	Inhibit Response Function*, Execution*
Disrupt process	Impair Process Control*, Execution*
Escape and evacuation	Evasion*

as to why the execution is (un)successful.

3) Tactical level: The tactical level of a D-APT attack ties the phases of the D-APT kill chain to the TTPs used during the attack, as seen in Figure 10. For this purpose a simplified OODA-loop is adapted to the cyber domain:

- *Observe:* taking in observations about the infrastructure and previous actions.
- *Orient:* put the observations into context, consisting of the current kill chain phase, the observed system and previous experience of the attacker.
- *Decide:* decide which TTP to execute next.
- *Act:* execute the TTP using the appropriate tool and return to observe.

In Table IV a mapping between the TTPs and the D-APT kill chain phases is given. The categories of TTPs given in ATT&CK ICS [46] are nearly sufficient to describe all phases of the D-APT kill chain, with two exceptions. First, the *weaponization and planning* phase can be populated with the TTPs described by Bahrami et al. [8] and by procedures from the DoD [27] [23]. The *rehearsal* phase can be described in four TTPs:

- Full replica testing, where the attacker is able to replicate the entire CI.
- Partial replica testing, where the attacker is able replicate parts of the entire CI.
- Emulated testing, where the attacker emulates the CIs specifications.
- Theoretical analysis, where the attacker can only theoretically infer the effects of the attack.

The relation of between the tactical and technical levels is quite simple: the execution of a D-APT is essentially a string of TTPs targeted at the infrastructure of the organisation.

4) Discussion: The presented D-APT model satisfies all criteria presented in Table II. It explicitly features two disruption actions, describes both lateral movement and the crucial pivoting phase, and includes rigorous preparation. In particular, the preparation includes target selection during *broad target selection* and a dedicated *rehearsal* phase. Another benefit of the model is it can describe the *escape and evacuation* actions of the attacker, which occur after the disruption is caused.

The presented model is more than a kill chain. The model combines the strategy, operations and tactics of an attacker. The strategic level in particular is typically absent from other kill chain or TTP oriented models. Furthermore, the model includes mental models of the attacker, in particular SA and OODA, as cornerstones of a D-APT. Finally, the presented model is designed to work together with the presented CI model, which is absent from existing kill chain models. All in all, the presented D-APT is a more extensive and specific description than existing APT models.

D. Qualitative evaluation

A qualitative evaluation of the proposed D-APT attack model is presented here by employing it on BlackEnergy3 (BE3), a well-studied D-APT with abundant available information; furthermore, the involved CP is quite general, hence the analysis can be adapted to other CPs. BE3 is considered to be one of the first attack of its kind, that is, a cyberattack disrupting a critical process. BE3 attack disrupted a subset of the Ukrainian electrical grid causing a 6 hour long blackout affecting hundred-thousands of people in 2015 [47]. BE3 is executed by Sandstorm who are typically attributed to Russia [48].

1) Critical infrastructure: The critical process disrupted by BE3 was *energy distribution* to households and fulfils a *social function*. This can be concluded from the damage reports citing 22500 customers losing power for 6 hours [47]. The

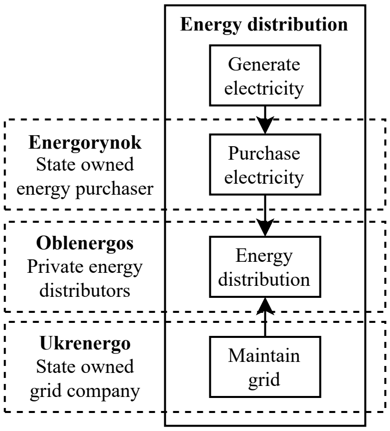

Fig. 11. Critical process of energy distribution broken down into critical business processes.

attack caused a disruption to the social order, but with limited economical and physical consequences.

Energy distribution in Ukraine can be dissected into critical business process executed by different organisations as shown in Figure 11. Energy is generated by a variety of companies who sell their energy to a single state owned organisation, from which the distribution companies (Oblenergos) purchase the energy they distribute to the households. Meanwhile the electrical grid is maintained by a single state owned organisation [49]. BE3 targeted three of the distribution companies, each of which serviced a local area limiting the scope of the attack.

On the technical level there was an IT network and an OT network. Crucially, the OT network was reachable from the IT network via a VPN [47]. The OT network consisted of several local substations where power is physically distributed. An operator's workstation controls the substations remotely through a substation gateway, which acts as a remote control choke-point. Each substation had a controllable circuit breaker, which is a piece of technology that literally breaks the electrical circuit thereby shutting down the flow of electricity.

2) D-APT attack: At the strategic level, this attacker has a high level of resources as they are at least able to develop or acquire custom firmware and malware. If Sandstorm is indeed attributable to Russia, then their motivations can include: 1) the protection of Russia's interests in Ukraine, specifically, to protect the ethnic Russians in Crimea [50] [47]; 2) retribution for a previous attack on the Russian controlled Crimean power grid [51]. The acceptable consequences can be inferred from the 2014 ceasefire agreement between Russia and Ukraine [52], which should not be violated. Note that attribution of cyberattacks is difficult and easily deniable, making it hard to claim violation of the ceasefire agreement. From these three factors we can conclude D-APTs are within in the feasible set of attacks. Indeed, Ukraine has been hit by the several more cyberattacks that disrupted Ukraine's electrical grid [53].

At the operational level we can analyse the attack using the D-APT kill chain, which is visually summarised in Figure 12. Each phase mentions (some of) the related TTPs; a full overview of these is given by MITRE [46].

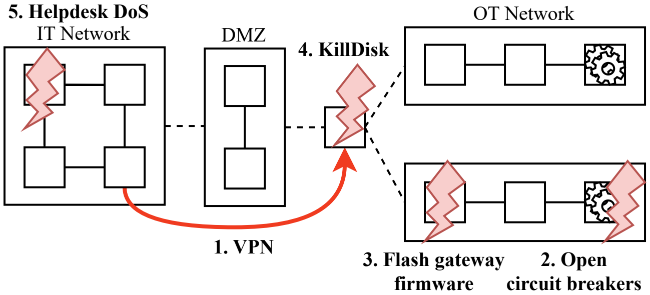

Fig. 12. Summary of the BE3 attack.

Broad target reconnaissance: At least 6500 cyberattacks were discovered in Ukraine, including the Red October attacks which targeted the energy sector for espionage [54] [48]. These attacks certainly added to the situational awareness of the attackers.

Specific target reconnaissance: The investigation of BE3 indicated a high level of coordination attributed to substantial reconnaissance activities [45]. The attackers maintained their presence in the network for six months, during which they must have performed very specific reconnaissance actions [55].

Weaponization and planning: During weaponization, a Word document was prepared with a BE3 dropper as a macro [56]. BE3 contained several plug-ins which needed to be prepared by the attacker [45].

Rehearsal: Each version of the BlackEnergy malware is an iteration on the previous and these have been used 'in the wild' before BE3, which can be considered partial testing [57]. The investigators concluded that the attacker must have had experts who knew the architecture, which indicates at least theoretical testing capabilities [58].

Intrusion and foothold: The attackers intruded the network through spear-phishing, which dropped the prepared Word document. They extracted valid credentials with which they could establish a foothold in the network through VPN [45].

Lateral movement & pivot: The valid credentials allowed the attackers to move through the network [57] and eventually it allowed them to pivot through the DMZ to the operator's workstation using a VPN.

Disrupt response: The attackers disrupted the response of the operators in two ways: they flashed the substation's gateway firmware such that commands made by the operator could not reach the substation [45] and they conducted a DoS attack against the distributors helpdesk such that customers could not signal the power outage [45].

Disrupt process The process disruption was simple: the attackers send the command to open the circuit breakers stopping the flow of electricity and causing an outage. This could not be undone remotely, as the operators could not send commands through the gateway [45].

Escape and evacuation: The attackers wiped the disk of the workstation using the KillDisk malware [45].

3) Discussion: This analysis features several advantages, as compared to other analyses using other models.

First, the combination of the CI and D-APT models enables a comprehensive and structured overview of the infrastructure and process. This puts the attack in context of the entire system and is an advantage over free-handed short descriptions of only the attacked parts of the infrastructure.

Another advantage is the strategic level description of the D-APT which provides a complete overview of the strategic considerations of the attacker. The strategic level describes the attacker's motivation, resources and tolerance and in this example shows that the attacker could execute similar attacks, which occurred a year later [59]. An overview of strategic considerations might be given, but this is typically relegated to the introduction of the attack [45]. The advantage of explicitly including these considerations as part of the model is that it allows the analysis to relate the strategy of the attacker to their operations and better understand the attack as a whole.

The D-APT kill chain gives a suitable overview of the attack. Without this kill chain crucial information would be lost. For example, the *broad target reconnaissance* through other cyberattacks or the rehearsal activities through previous versions of BlackEnergy could not be incorporated. Furthermore, the disruption steps of the attack are well described using the two disruption phases, as is the deletion of evidence through the *escape and evacuation* step. These three activities would in other kill chains be hidden in "actions on objectives".

Finally, we must address the completion of this analysis, that is, whether it describes all aspects of the attack. As the analysis uses a model and all models are an abstraction of reality, the analysis is almost definitionally incomplete. However, this analysis describes more facets of the attack compared to other kill chain based analyses, in particular regarding disruption, reconnaissance and rehearsal. A drawback of this model is that it abstracts over the most technical details of the attack, such as the specific malware-code, by using TTPs as its building blocks.

V. Application: incident reporting

This section discusses the data availability problem, that is, published reports are not *consistent* and security vendors have a *monopoly* on primary source data. This section describes an architecture that makes a small step forward in the consistency aspect of the data availability problem.

Data about cyberattacks basically come in two varieties: threat intelligence and incident reporting. Threat intelligence focusses on current threats, while incident reporting focusses on what has happened when a threat became an attack. The de facto standard language to share threat intelligence is Structured Threat Information eXpression (STIX) [60]. While STIX is a mandatory standard in some countries to share threat intel [61], no such standard exists for incident reporting. Providing a standard for incident reporting would help the consistency problem. We propose an extension to STIX to facilitate structured incident reporting, as STIX is already widely adopted and because introducing a new standard is rarely the correct solution.

The STIX extension consists of one custom object and a few custom fields in existent objects. Starting with the latter, we add fields for critical (business) process and societal functions to the STIX Domain Object `infrastructure`, fields to record the (sub) sector and attributed nationality to `identity`. To `threat_actor` we add a field for attributed nationality, tolerance and acceptable consequences. We define a STIX Custom Object `x_incident` containing fields for the start and end date, initiating incidents, cause, consequence, damages, impact, etc. Essentially this object contains values for all concepts on the strategic, societal, operational and process level of the models presented in Section IV. The technical and tactical level of the model can be shared via STIX natively. A more detailed description is given in Appendix A.

Using the STIX specification, incident information can be shared between organisations using Trusted Automated eXchange of Indicator Information (TAXII) [62], which is a standard to share STIX messages. With access to such a network, a simple database design could capture all incident reports and making these available to researchers with minimal human effort. A relational database schema is given in Figure 13, which is an extension of the design used by Van Eeten et al. [6]. The schema is designed to, in addition to storing information about regular CI incidents, store information about D-APTs as well. The schema contains tables of the previous iteration of the database, except normalised to 3rd normal form. It contains static tables, which only contain a taxonomy to specify the incident e.g. different values for locality. The rest of the schema are added tables based on the models proposed in this paper.

While there are major limitations to this approach, most dominantly willingness from industry to participate, the prospect of no more manual processing [6] of incident information is quite enticing.

VI. Discussion and limitations

The presented model is a novel holistic approach to D-APTs by describing the strategic, operational and tactical level of an attack and relating these to the technical, process and societal level of critical infrastructure. The approach is largely a consequence of adapting the levels of warfare to the cyber domain. The resulting model describes the entire attack and is therefore suitable for structured incident reporting. For contrast, existent attack models only describe either the tactical level or an operational kill chain. The basis of the model lies in established theory. The attack section is based on military theory or real world evidence, while the CI section is based on well-established industry concepts. In general, the model uses strong established concepts and combining them in a novel way.

The model gives a unique insight into the operations of the attacker. First of all, the model is rooted in military theory and doctrine, which is the closest publicly available insight

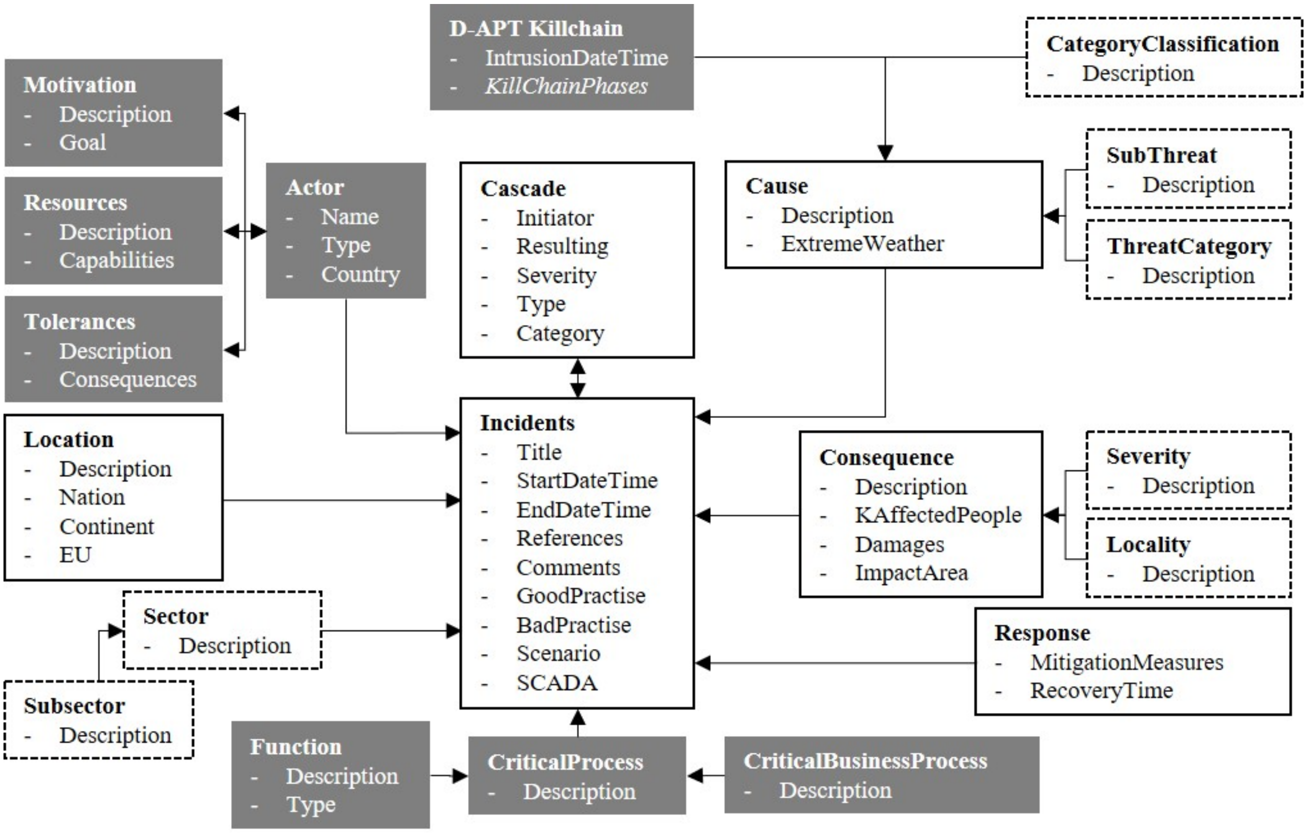

Fig. 13. Proposed database schema to capture D-APT incident. The boxes with a white background depict normalised existing tables, the boxes with dashed borders depict static tables and the boxes with a grey background depict added tables.

into real world sophisticated cyber operations. Secondly, the additional description of the attacker's mental state gives insight into their operations. The link between the operational and tactical level through the OODA-loop is quite natural, but hard to verify in practise. Situational awareness describes when a phase can successfully be concluded, although it should be noted that this works best during the reconnaissance and other preparation phases. Additionally, the connection between attack and impact is made explicitly by describing both the attacker and the defender in detail.

Compared to other models, the D-APT model differs in a number of ways. By narrowing the scope to D-APT attacks only, the model makes a trade-off in being less flexible and more specific. There consequences are numerous: the D-APT model features disruption steps, which are more suitable in a D-APT, but lack the flexibility of the "action on objectives" step of the CKC. Compared to other kill chains, the D-APT model emphasises reconnaissance which gives more focus on increasing situational awareness. Another difference with other models is that the D-APT model includes rehearsal, for which it gives a simple taxonomy. The inclusion of rehearsal and disruption, with emphasis on reconnaissance are an advantage as compared to other models.

The primary limitation of the methodology is the absence of empirical data to quantitatively validate the results. This is a problem in the entire field [1], but especially in the limited scope of D-APT attacks there are only few well-documented examples: Stuxnet, BlackEnergy3 and Industroyer. The other two well-known ICS attacks Havex and TRITON are unsuitable as they do not involve critical infrastructures. This is counteracted by meticulously finding evidence for any of the claims made in this paper and picking the most suitable use case. BE3 involves a highly sophisticated attacker, a non-trivial critical process and despite occurring quite recently, has received tremendous academic scrutiny.

VII. Conclusion and Future Work

In this paper we have presented a novel model describing Disruptive APT attacks targeting critical infrastructure. The model 1) describes the defenders' infrastructure, processes and societal functions; 2) describes the attackers' strategic considerations, operations and tactics. The model is based on military theory and existent models. The validation is conducted qualitatively against a known use-case. Finally, the result is shown to be applicable to incident reporting, to which end an extension to STIX is presented.

Some interesting directions for future work include engineering an operational incident database as incident reporting tool using this model. This is a non-trivial task from a process perspective: organisation's willingness to supply access to their data on cyber incidents might be low, hence alternate sources of information must be found. Another future topic is to investigate the combination of a D-APT with natural disasters. BE3 “only” caused 6 hours of outage, which is a fairly minimal effect especially when considering the sophistication of the attack. Perhaps this effect can be amplified if the attack occurred during a natural disaster. This would fit the pattern of D-APT as the attacker can remain in the network to strike at the right moment. Finally, the practical implementation of the kill chain can be improved. It takes months to execute a D-APT attack [34], which limits is use from an attacker’s perspective. In contrast, it takes 12 minutes to execute current kill chains from scanning a target to bombing it [28]. If cyber operations are to be involved in war, then the D-APT kill chain needs to be executed faster.

References

[1] A. Lemay, J. Calvet, F. Menet, and J. Fernandez, “Survey of publicly available reports on advanced persistent threat actors,” *Computers & Security*, vol. 72, 2017.

[2] R. Khan, P. Maynard, K. McLaughlin, D. M. Laverty, and S. Sezer, “Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid,” in *ICS-CSR*, 2016.

[3] N. Virvilis and D. Gritzalis, “The big four - what we did wrong in advanced persistent threat detection?” 2013, pp. 248–254.

[4] Ministerie van Justitie en Veiligheid, “Overzicht vitale processen,” https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen, 2020, [Accessed: 2020-09-23].

[5] H. Luiijf and A. Nieuwenhuijs, “Extensible threat taxonomy for critical infrastructures,” *International journal of critical infrastructures*, vol. 4, no. 4, pp. 409–417, 2008.

[6] M. Eeten, A. Nieuwenhuijs, E. Luiijf, M. Klaver, and E. Cruz, “The state and the threat of cascading failure across critical infrastructures: The implications of empirical evidence from media incident reports,” *Public Administration*, vol. 89, p. 381, 2011.

[7] E. Hutchins, M. Cloppert, and R. Amin, “Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains,” *Leading Issues in Information Warfare & Security Research*, vol. 1, 2011.

[8] P. N. Bahrami, A. Dehghantanha, T. Dargahi, R. M. Parizi, K.-K. R. Choo, and H. H. Javadi, “Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures.” *Journal of Information Processing Systems*, vol. 15, no. 4, 2019.

[9] C. Simmons, C. Ellis, S. Shiva, D. Dasgupta, and Q. Wu, “Avoidit: A cyber attack taxonomy,” in *9th Annual Symposium on Information Assurance (ASIA’14)*, 2014, pp. 2–12.

[10] M. J. Egan, “Anticipating future vulnerability: Defining characteristics of increasingly critical infrastructure-like systems,” *Journal of contingencies and crisis management*, vol. 15, no. 1, pp. 4–17, 2007.

[11] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, “Identifying, understanding, and analyzing critical infrastructure interdependencies,” *IEEE control systems magazine*, vol. 21, no. 6, pp. 11–25, 2001.

[12] P. Reidy, “Combating the insider threat at the fbi,” *Blackhat USA*, 2013.

[13] C. Alcaraz and S. Zeadally, “Critical infrastructure protection: Requirements and challenges for the 21st century,” *Int. J. Crit. Infrastructure Prot.*, vol. 8, pp. 53–66, 2015.

[14] M. Brunner, H. Hofinger, C. Krauß, C. Roblee, P. Schoo, and S. Todt, “Infiltrating critical infrastructures with next-generation attacks,” *Fraunhofer Institute for Secure Information Technology (SIT), Munich*, 2010.

[15] J. D. Howard and T. A. Longstaff, “A common language for computer security incidents,” Sandia National Labs., Albuquerque, NM (US), Tech. Rep., 1998.

[16] S. Hansman and R. Hunt, “A taxonomy of network and computer attacks,” *Computers & Security*, vol. 24, pp. 31–43, 2005.

[17] M. Uma and G. Padmavathi, “A survey on various cyber attacks and their classification.” *IJ Network Security*, vol. 15, no. 5, pp. 390–396, 2013.

[18] K. C. Desouza, A. Ahmad, H. Naseer, and M. Sharma, “Weaponizing information systems for political disruption: The actor, lever, effects, and response taxonomy (alert),” *Computers & Security*, vol. 88, p. 101606, 2020.

[19] M. Ussath, D. Jaeger, F. Cheng, and C. Meinel, “Advanced persistent threats: Behind the scenes,” *2016 Annual Conference on Information Science and Systems (CISS)*, pp. 181–186, 2016.

[20] O. Thonnard, L. Bilge, G. O’Gorman, S. Kiernan, and M. Lee, “Industrial espionage and targeted attacks: Understanding the characteristics of an escalating threat,” in *Research in Attacks, Intrusions, and Defenses*, D. Balzarotti, S. J. Stolfo, and M. Cova, Eds. Springer Berlin Heidelberg, 2012, pp. 64–85.

[21] P. Chen, L. Desmet, and C. Huygens, “A study on advanced persistent threats,” in *IFIP International Conference on Communications and Multimedia Security*. Springer, 2014, pp. 63–72.

[22] W. Tirenin and D. Faatz, “A concept for strategic cyber defense,” in *MILCOM 1999. IEEE Military Communications. Conference Proceedings (Cat. No. 99CH36341)*, vol. 1. IEEE, 1999, pp. 458–463.

[23] Department of Defense, US, “Cyberspace operations,” 2018.

[24] M. R. Endsley, “Toward a theory of situation awareness in dynamic systems,” in *Situational awareness*. Routledge, 2017, pp. 9–42.

[25] S. Jajodia, P. Liu, V. Swarup, and C. Wang, *Cyber Situational Awareness*, ser. 46. Springer, 2010, vol. 46.

[26] A. Ahmad, J. Webb, K. C. Desouza, and J. Boorman, “Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack,” *Computers & Security*, 2019.

[27] Department of Defense, US, “Joint targeting,” 2013.

[28] J. A. Tirpak, “Find, fix, track, target, engage, assess,” https://www.airforcemag.com/article/0700find/, 2000, [Accessed: 2020-03-09].

[29] A. Hayes, “Defending against the unknown: Antiterrorism and the terrorist planning cycle,” http://www.jcs.mil/content/files/2009-04/041309155243_spring2008.pdf, 2008, [Accessed: 2020-03-24].

[30] J. R. Boyd, “The essence of winning and losing,” http://pogoarchives.org/m/dni/john_boyd_compendium/essence_of_winning_losing.pdf, 1992, [Accessed: 2020-05-22].

[31] W. Voster, P. Bloemen, M. Beumer, H. Mathijssen, and A. Dekker, “Cyber security supply chain risicoanalyse,” https://www.cybersecurityraad.nl/binaries/Cybersecurity_supply_chain_risico-analyse_DEF_tcm107-314472.pdf, 2015, [Accessed: 2020-06-08].

[32] T. J. Williams, “The purdue enterprise reference architecture,” *Computers in Industry*, vol. 24, no. 2, pp. 141 – 158, 1994.

[33] B. D. Bryant and H. Saiedian, “A novel kill-chain framework for remote security log analysis with siem software,” *Comput. Secur.*, vol. 67, pp. 198–210, 2017.

[34] S. Malone, “Using an expanded cyber kill chain model to increase attack resiliency,” https://www.blackhat.com/docs/us-16/materials/us-16-Malone-Using-An-Expanded-Cyber-Kill-Chain-Model-To-Increase-Attack-Resiliency.pdf, 2016, [Accessed: 2020-03-31].

[35] Mandiant, “Apt1 exposing one of china’s cyber espionage units,” 2013, [Accessed: 31-03-2020].

[36] J. Rutherford and G. B. White, “Using an improved cybersecurity kill chain to develop an improved honey community,” *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pp. 2624–2632, 2016.

[37] H. Kim, H. Kwon, and K. K. Kim, “Modified cyber kill chain model for multimedia service environments,” *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 3153–3170, 2019.

[38] “The industrial control system cyber kill chain,” https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297, 2015, [Accessed: 2020-09-01].

[39] “MITRE ATT&CK™ Enterprise,” https://attack.mitre.org/matrices/enterprise/, [Accessed: 2020-04-01].

[40] P. Pols, “The unified kill chain: Designing a unified kill chain for analyzing, comparing and defending against cyber attacks,” *Cyber Security Academy*, 2017.

[41] “Vault 7: Cia hacking tools revealed,” https://wikileaks.org/ciav7p1/, 2017, [Accessed: 2020-08-27].

[42] “Kim jong un has quietly built a 7,000-man cyber army that gives north korea an edge nuclear weapons don’t,” 2020.

[43] Securelist, ““Red October” Diplomatic Cyber Attacks Investigation,” https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/#4, 2013, [Accessed: 2020-09-02].

[44] Mark Goudie, “Going Beyond Malware: The Rise of “Living off the Land” Attacks,” https://www.crowdstrike.com/blog/going-beyond-malware-the-rise-of-living-off-the-land-attacks/, 2019, [Accessed: 2020-09-02].

[45] T. C. Robert M. Lee, Michael J. Assante, “Analysis of the cyber attack on the ukrainian power grid,” https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, 2016, [Accessed: 2020-06-08].

[46] “Mitre att&ck ™ics,” https://collaborate.mitre.org/attackics/index.php/Main_Page, [Accessed: 2020-04-01].

[47] K. Zetter, “Inside the cunning, unprecedented hack of ukraine’s power grid,” https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, 2016, [Accessed: 2020-07-21].

[48] Malpedia, “Sandworm,” https://malpedia.caad.fkie.fraunhofer.de/actor/sandworm, [Accessed: 2020-07-21].

[49] I. A. Vitaliy Radchenko, Olexander Martinenko, “Cms guide to electricity - ukraine,” https://www.lexology.com/library/detail.aspx?g=c722c0f8-c3b8-4a42-b129-031eed1dc2a6, 2015, [Accessed: 2020-07-21].

[50] J. Percha, “Transcript: Putin says russia will protect the rights of russians abroad,” https://www.washingtonpost.com/world/transcript-putin-says-russia-will-protect-the-rights-of-russians-abroad/2014/03/18/432a1e60-ae99-11e3-a49e-76adc9210f19_story.html, 2014, [Accessed: 2020-07-21].

[51] D. M. Herszenhorn, “Kiev blamed for blackout in capital of crimea,” https://www.nytimes.com/2014/03/25/world/europe/ukraine-pulls-all-its-forces-out-of-crimea.html, 2014, [Accessed: 2020-07-21].

[52] Organization for Security and Co-operation in Europe, “Press statement by the trilateral contact group,” https://www.osce.org/home/123124, 2014, [Accessed: 2020-07-21].

[53] Council on Foreign Relations, “Global conflict tracker - cyberoperations,” https://www.cfr.org/cyber-operations/, [Accessed: 2020-07-22].

[54] N. Zinets, “Ukraine hit by 6,500 hack attacks, sees russian ’cyberwar’,” https://www.reuters.com/article/us-ukraine-crisis-cyber/ukraine-hit-by-6500-hack-attacks-sees-russian-cyberwar-idUSKBN14I1QC, 2016, [Accessed: 2020-07-21].

[55] P. Polityuk, “Ukraine sees russian hand in cyber attacks on power grid,” https://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VL18E, 2016, [Accessed: 2020-07-21].

[56] GReAT, “Blackenergy apt attacks in ukraine employ spearphishing with word documents,” https://securelist.com/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/73440/, 2016, [Accessed: 2020-07-21].

[57] S. Shrivastava, “Blackenergy - malware for cyber-physical attacks,” https://itrust.sutd.edu.sg/wp-content/uploads/sites/3/2016/10/itrust-analysis-blackenergy.pdf, 2016, [Accessed: 2020-06-08].

[58] S. J. Pavel Polityuk, Oleg Vukmanovic, “Ukraine’s power outage was a cyber attack: Ukrenergo,” https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA, 2016, [Accessed: 2020-07-21].

[59] Catalin Cimpanu, “Security researchers find solid evidence linking Industroyer to NotPetya,” https://www.zdnet.com/article/security-researchers-find-solid-evidence-linking-industroyer-to-notpetya/, 2018, [Accessed: 2020-09-22].

[60] “Stix™version 2.1,” https://docs.oasis-open.org/cti/stix/v2.1/cs01/stix-v2.1-cs01.html, 2020, [Accessed: 2020-08-14].

[61] “Stix en taxii,” https://www.forumstandaardisatie.nl/open-standaarden/stix-en-taxii, 2017, [Accessed: 2020-08-20].

[62] “Taxii™version 2.1,” https://docs.oasis-open.org/cti/taxii/v2.1/cs01/taxii-v2.1-cs01.html, 2020, [Accessed: 2020-08-17].

Appendix A
DB Schema and STIX specification

This section presents two products derived from the model presents a STIX design to capture structured critical information incidents data. As most information regarding D-APTs is already captured in STIX, a custom object and a few custom fields suffice for a standardised capture of information about D-APTs. The remainder of this section gives a specification for these objects and fields that comply with the STIX standard. An additional benefit of capturing D-APTs in a STIX specification, is that this automatically allows the information to be shared using Trusted Automated eXchange of Indicator Information (TAXII) [62].

The STIX Custom Object (SCO) `x_incident` is described in Table V. The entire table is an SCO, as indicated by the “x_” prefix. The column *origin of field* describes what database table the field comes from or whether it is automatically included by STIX ()required/optional). By default all custom fields are optional. The field name and type describe the field.

In the STIX Domain Objects (SDO) the *italicised* fields are custom fields, as also indicated by the “x_” prefix. The specifications for the SDOs `infrastructure`, `identity` and `threat_actor` are given in Table VI, VII and VIII respectively.

TABLE V
Specification SCO x_incident

Origin of field	Field name	Definition
Required	type	Type of this object
Required	id	Unique identifier, follows format
Required	spec_version, created, modified	Default required SDO values
Optional	created_by_ref, revoked, labels, confidence, lang, object_marking_refs, granular_markings	Default optional SDO values
Optional	external_references	List of external references
Incident	x_title	String with incident name
Cascade	x_initiator_incident	String with ID of initiator incident in a cascade
Cause	x_cause_description	String describing the cause of incident
Consequence	x_consequence_description	String describing the consequence of incident
Consequence	x_k_affected_people	integer of number of affected people / 1000
Consequence	x_damages	integer estimated damages in euros
Consequence	x_impact_area	String describing the impact area
Severity	x_severity	String describing the severity of incident { low, very weak, weak, medium, potentially high, high}
Locality	x_locality	String describing the locality of incident { very local, local, island wide, regional, nation wide, Europe, Europe scale, international worldwide, global}
Response	x_mitigation_measures	String describing the mitigation measure taken bij the actor
Incident	x_comments	String giving author comments
D-APT Killchain	x_intrusion_date_time	Strings depicting: date of first intrusion
Incident	x_start_data_time	date of the start of the incident
Incident	x_end_data_time	date of the end of the incident
Response	x_recovery_time	time it took to recover from the incident
Incident	x_good_practise	Boolean, does the incident include
Incident	x_bad_practise	Boolean, does the incident include
Incident	x_scenario	Boolean, does the incident include
Incident	x_scada	Boolean, does the incident involve
Cause	x_common_cause_failure	Boolean, does the incident involve
Cause	x_extreme_weather	Boolean, does the incident involve
Cause	x_category_classification	String, single term description of the problem
Cause	x_threat_category	String, follows VITAAL threat classification
Cause	x_sub_threat	String, follows VITAAL threat classification

TABLE VI
Specifcaton SDO infrastructure

Origin of field	Field name	Definition
Required	type	Type of this SDO
Required	id	Unique identifier, follows format
Required	spec_version, created, modified	Default required SDO values
Optional	created_by_ref, revoked, labels, confidence, lang, object_marking_refs, grannular_markings	Default optional SDO values
Optional	external_references	List of external references
Optional	description	String describing the attacked infrastructure
CriticalProcess	*x_critical_process*	*String describing the involved critical process*
CriticalBusinessProcess	*x_critical_business_process*	*String describing the involved critical business process*
SocietalFunction	*x_societal_function*	*String describing the societal function performed by the critical process*

TABLE VII
Specifcaton SDO identity

Origin of field	Field name	Definition
Required	type	Type of this SDO
Required	id	Unique identifier, follows format
Required	spec_version, created, modified	Default required SDO values
Optional	created_by_ref, revoked, labels, confidence, lang, object_marking_refs, granular_markings	Default optional SDO values
Optional	external_references	List of external references
Required	name	Name of identity
Optional	role	Role of this actor {victim, owner}
Optional	sector	Industry this identity belongs to, follows EU list
SubSector	*x_subsector*	*Sub sector to which this identity belongs*
Actor	*x_nation*	*Nation the identity is attributed to*

TABLE VIII
SPECIFCATON SDO THREAT_ACTOR

Origin of field	Field name	Definition
Required	type	Type of this SDO
Required	id	Unique identifier, follows format
Required	spec_version, created, modified	Default required SDO values
Optional	created_by_ref, revoked, labels, confidence, lang, object_marking_refs, granular_markings	Default optional SDO values
Optional	external_references	List of external references
Required	name	Name of identity
Actor	*x_nation*	*Nation the identity is attributed to*
Optional	primary_motivation	String of motivation of actor, defined in open vocabulary
Optional	goals	List of high level goals, defined in open vocabulary
Optional	resource_level	String of resource level, defined in open vocabulary
Optional	sophistication	String of capabilitiy level, defined in open vocabulary
Tolerance	*x_tolerance*	*String describing the tolerance level of the attacker*
Tolerance	*x_acceptable_consequences*	*String describing acceptable consequences to the attacker*