Juhani Merilehto

IT ARMY OF UKRAINE AS COMPLEX ADAPTIVE SYSTEM

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Merilehto, Juhani
Ukrainan IT-Armeija Kompleksisena Adaptiivisena Järjestelmänä
Jyväskylä: Jyväskylän yliopisto, 2023, 67 s.
Turvallisuus ja Strateginen analyysi, pro gradu -tutkielma
Ohjaaja(t): Lehto, Martti

Tämä tutkielma tarkastelee Ukrainan IT-Armeijan (ITAU) toimintoja ja ominaisuuksia Kompleksisten Adaptiivisten Järjestelmien (CAS) teorian näkökulmasta. ITAU, ad-hoc-tyyppinen valtion tukema kybertoimija, tarjoaa erinomaisen tapauksen siitä, miten tällaiset ryhmät toimivat nopeasti kehittyvässä kybersodankäynnin maisemassa. Pääasiallinen tutkimuskysymys tutkii CAS:n ominaisuuksia, joita voidaan löytää ITAU:sta. Tukikysymysten kautta syvennymme erityisiin ominaisuuksiin, kuten sopeutumiseen, epälineaarisuuteen, emergenssiin, itseorganisoitumiseen, palautteeseen, monimuotoisuuteen, yhteistyöhön, viestintään, yhteisevoluutioon ja kontekstuaalisuuteen. Analyysi paljastaa, että ITAU osoittaa keskeisiä CAS:n ominaisuuksia, kuten sopeutumisen nopeasti muuttuviin olosuhteisiin, kollektiivisen kyvykkyyden kyberulottuvuudessa, ja oppimiskyvyn joka mahdollistaa ryhmän toiminnan jatkumisen muuttuvissa ja kehittyvissä olosuhteissa. Tämä tutkimus edistää kybersodankäynnin kirjallisuutta tarjoamalla yksityiskohtaisia näkemyksiä ITAU:n toiminnoista ja osoittamalla CAS-teorian soveltuvuuden kyberryhmien analyysiin. Analyyttisen linssin käytettävyys osoittaa sen, että sitä voitaisiin käyttää analysoimaan ja ymmärtämään vastaavan kaltaisia ryhmittymiä, joita voi ilmetä tulevaisuudessa.

Asiasanat: Kybersodankäynti, Kompleksinen adaptiivinen järjestelmä, Joukkoistaminen, Ukrainan IT-Armeija

ABSTRACT

Merilehto, Juhani
IT Army of Ukraine as Complex Adaptive System
Jyväskylä: University of Jyväskylä, 2023, 67 pp.
Security and Strategic analysis, Master's thesis
Supervisor: Lehto, Martti

This thesis explores the activities and properties of the IT Army of Ukraine (ITAU) through the lens of Complex Adaptive Systems (CAS) theory. As an ad-hoc state sponsored cybergroup, the ITAU provides a compelling case study for understanding how such groups operate in the rapidly evolving landscape of cyberwarfare. The primary research question investigates the characteristics of CAS that can be found in the ITAU. Through supporting questions, we delve into specific attributes such as adaptation, nonlinearity, emergence, self-organization, feedback, diversity, cooperation, communication, co-evolution, and contextuality. The analysis reveals that the ITAU exhibits key CAS characteristics, including adaptation to rapidly changing conditions, the emergence of collective cyber-capabilities and learning that allows the group to continue functioning in changing and evolving circumstances. This study contributes to the literature on cyberwarfare by offering detailed insights into the operations of the ITAU and demonstrating the applicability of CAS theory to the analysis of cybergroups. The usability of the analytical lens can have practical implications, suggesting that it could be used for understanding and responding to similar groups that may emerge in the future.

Keywords: Cyberwarfare, Complex Adaptive System, Crowdsourcing, IT Army of Ukraine

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

The War in Ukraine that started in 2014, escalated into full-scale conventional war between nation states of Russia and Ukraine in 24th of February 2022. The escalation of the war received widespread condemnation, ranging from political statements (UN News, 2022) to volunteer civil action and massive corporate withdrawal (Yale School of Management, 2023) from Russia. However, events transpired also in the cyber-domain: new cyber-groups were formed due to the war and old groups stated their affiliation to either being in support of either nation or proclaiming neutrality. During the research conducted in this thesis it was apparent that active cybergroups that publicly stated or by evident actions were taking at least some part in the Russo-Ukrainian war were numbered over 80.

One notable cyber-group which arose in response to the Russian aggression was the IT Army of Ukraine (ITAU). The birth of this group is largely attributed to the Ukrainian Minister of Digital Transformation Mykhailo Fedorov, who posted to Twitter, Facebook, and Telegram on the creation of an IT Army (Mykhailo, 2022). His posts and the first message to the official Telegram channel of the group can be summed as a call for anyone with any cyber-capabilities to fight by using any attack vector possible against Russia. The largest and most visible part of the group and its actions are the crowdsourced Distributed Denial-of-Service attacks against targets in the Russian society at large, which are coordinated via dedicated Telegram channel.

As the war in Ukraine has progressed, so has the group evolved. Some aspects of the group have changed more subtly, during a longer period of time and some are simple changes that have had influence on the nature and impact of the entire group. The nature of the group being largely an open system (Pondy & Mitroff, 1979) through its Telegram channel, gives an opportunity to conduct research for an extended period to understand how this type of a massive cybergroup evolves, coordinates its activity, self-organizes, and co-evolves with its operating environment (Buckley, 1968).

This thesis is an ethnography-oriented case study (Côté-Boileau et al., 2020) of the IT Army of Ukraine (ITAU), utilizing Complex Adaptive Systems (Buckley, 1968; Holland, 1995) as a theoretical and analytical lens. The purpose of this research is to gain insight into the IT Army of Ukraine, and specifically how it as a Complex Adaptive System conducts Cyberwarfare operations. To achieve this, a research question (RQ) was formed, along with supporting questions (SQ):

RQ1: What are the characteristics of CAS that can be found in ITAU?

SQ1: How do the principles of adaptation and self-organization manifest in ITAU's response to changing conditions?

SQ2: In what ways do emergent properties and nonlinearity characterize ITAU's operations?

SQ3: How does ITAU utilize feedback mechanisms and display diversity among its components?

SQ4: What evidence is there of cooperation and communication within ITAU?

SQ5: How do the principles of openness and contextuality manifest in ITAU's activities?

SQ6: How does co-evolution manifest in ITAU and adjacent systems?

The motivation for this study is to produce insights from ITAU, as it currently stands out due to its state-affiliation, massive size, persistency, crowdsourced nature, and the context it has emerged from. These insights could be used in further studies of such groups, especially if this type of activity is a cue for future trend in the cyber domain. The use of CAS as an underlying theory also contributes to the literature of Complexity Science, as it has thus far been scarcely used in analyzing cybergroups or cyberwarfare.

2 THEORETICAL FRAMEWORK

The theoretical underpinnings of this thesis are twofold. First, we explore the relevant literature pertaining to the cyber-domain. This involves delving into the intricate and often ambiguous realm of Cyber War and Cyber warfare. Additionally, we will shed light on various Cyber groups, showcasing their roles as significant actors within this space. Second, we turn our attention to the actual theoretical lens employed in this study: Complex Adaptive Systems. To fully appreciate this perspective, we will deep dive into the domain of Complexity Science. This framework allows for a comprehensive understanding of the multi-dimensional dynamics at play in the IT army of Ukraine.

2.1 On Cyber War and Cyber warfare

This chapter aims to provide a comprehensive understanding of the concepts of Cyber War and Cyber Warfare, discussing their definitions, characteristics, and challenges in the current literature. Cyber warfare and Cyber war are terms that currently lack conceptual clarity, and despite the increasing literature and relevance towards the subject, no unanimous concept has yet to emerge (Andress & Winterfeld, 2014, p. 3; Hughes & Colarik, 2017). Also, terms Cyber war and cyber warfare have often been used synonymously (Hughes & Colarik, 2017, p. 29). In this thesis, the term Cyber war is used in similar fashion where *war*, is to mean state of war, or an event (i.e., the Second World War). Thus, Cyber warfare is meant to describe more the activity of conducting war and as a verb. The definitions of Cyber warfare vary by source and author (Hughes & Colarik, 2017, p. 26), which brings a layer of ambiguity to the field, and brings challenges in representing the various definitions of different authors. In the following paragraphs, there are some highly cited definitions on the concepts of cyber war and cyberwarfare.

According to Clarke and Knake (2011, p. 9), cyber warfare is the "*act of a nation state penetrating another nation's computer or network to cause damage or disruption*", which as a definition gives quite wide conceptual maneuverability. On the other hand, Arquilla and Ronfeldt (1993) define it as *conducting military operations according to information-related Security Studies principles* – and differentiating "netwar" from it as a distinct type, encompassing it into more to the civilian perspective as well as of information and influencing operations. Authors such as Nye (2011) also describe Cyberwar mainly from the viewpoint of military operations, as a type of "*hostile actions in cyberspace that aim to amplify or have direct major and violent kinetic effects*".

Some authors take the road of reflecting Cyber warfare and Cyber war through historically dominant – or at least well-known – definitions of war and warfare, such as von Clausewitz and Sun Tzu. Shakarian et al. (2013) look at the Clausewitz's famous definition of war being "an extension of policy by other means" and replace the other means with 'actions taken in cyber space' (p.2). They also extend the definition to consider threat levels and nonstate actors, and articulate their definition as: "*Cyber war is an extension of policy by actions taken in cyber space by state or nonstate actors that either constitute a serious threat to a nation's security or are conducted in response to a perceived threat against a nation's security.*" (2013, p. 2).

Contrary to several other authors, Andress and Winterfeld (2014) do not try to define Cyber Warfare concisely, instead of laying out multiple definitions of what *cyber,* and *warfare* constitutes (p. 3-4). In their *defining* of the term they use Clausewitz, but also Sun Tzu – to articulate that if the term warfare is to be used, it should be specifically the traditional military perspective; in similar vein they do not define cyber themselves, but introduce multiple different definitions from various sources (p. 3-4). In essence, this acts out as an example of the ambiguousness of the term itself.

Continuing, Andress and Winterfeld (2014), as per military tradition, make further note of articulating the different levels of warfare; the *tactical* level, where individual 'battles' are conducted to achieve goals by tactical units, the *operational* level where multiple battles are combined into campaigns and linking tactics to strategy, and the *strategic* level where nation or nation-coalitions enforce the aspiration of national political goals (p. 5). In a more sophisticated manner, Lehto and Henselmann (2020) articulate the levels of warfare through five-level approach, seeing the level of Grand Strategy to be the State level, while Strategy encompasses the level of Armed Forces, with Operational level seeing the deployment to theaters of war to accomplish strategic goals, and tactical level being articulated as series of cyber operations. The fifth level describes the term "Superiority", where the degree of dominance over opposing force is measured (Lehto & Henselmann, 2020, p. 323).

Authors such as Hunker (2010) take perhaps less militaristic perspective, however still connecting the concept of "use-of-force" with it, by defining Cyber warfare as "*…a serious form of disruptive cyber attack by a nation on another nation's cyber space, crossing the line into being considered a use of force.*" (p.4). Comparing this to Rid Thomas (2012) definition, which also connects Cyberwar to the physical domain and use-of-force, and describes it however more as a *potentially* lethal act of force conducted through malicious code.

Schaap et al. (2009, p. 127) describes Cyberwar as using "*network-based capabilities to disrupt, deny, degrade, manipulate or destroy information resident in computers and computer networks or the computers and networks themselves of another state.*" Nicholson et al. (2012, p. 421) uses a 2001 US Congressional Research Service Report (Hildreth, 2001) on to inform their definition of "Cyber-Warfare", being "*attacks and defense issued by nation states that take place over networks rather than by physical means.*"

Some institutions, such as the RAND Corporation, summarize Cyber Warfare as the "*actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.*" (RAND Corporation, 2023). This definition by RAND is introduced to bring some comparison to the quite wide terminology used by academic authors – RAND goes into specifics such as DoS attack as an example tactic, and interestingly including *international organization* into the attacking perspective. The different definitions by authors can be seen in Table 1.

Table 1 Definitions of Cyber war and Cyber warfare

Definition	**Source**
Actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.	RAND Corporation (2023)
Cyber war is an extension of policy by actions taken in cyber space by state or nonstate actors that either constitute a serious threat to a nation's security or are conducted in response to a perceived threat against a nation's security.	Shakarian et al. (2013)
The use of network-based capabilities of one state to disrupt deny degrade manipulate or destroy information resident in computers and computer networks or the computers and networks themselves of another state.	Nicholson et al. (2012)
A potentially lethal, instrumental, and political act of force conducted through malicious code.	Rid Thomas (2012)
Cyber war is the act of nation state to penetrate another nation's computer or network in order to cause damage or disruption.	Clarke, R. A. & Knake, R. K. (2011)
Hostile actions in cyberspace that have effects that amplify or are equivalent major kinetic violence.	Nye Jr J.S. (2011)
Cyber warfare is a serious form of disruptive cyber-attack by a nation on another nation's cyber space, crossing the line into being considered a use of force.	Hunker, J. (2010)
Hostile actions in cyberspace that are likely to have a significant effect on the safety or security of another state or produce a significant loss of functionality or capability on target system(s).	Schaap, A. J. (2009)
Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related Security Studies principles.	Arquilla, J. & Ronfeldt, D. (1993)

When examining the definitions of Cyberwarfare, the concept of attribution is important to consider. The fact that the ITAU is inherently a volunteer organization, makes its state-affiliation more ambiguous than if it were a formal part of the Ukrainian military, as an example. While it is evident that there is at least some coordination and cooperation between the state of Ukraine and the ITAU, it is difficult to label it as state-actor, but more as being a state-sponsored actor (Lucas, 2014). Through this lens, one can start to reflect if the ITAU is in fact, conducting cyberwarfare – if cyberwarfare is state-on-state activity, and ITAU is deemed not to be part of the state, then in principle its activities are basically hacking and hacktivism. When looking at the definition by Arquilla and Ronfeldt (1993), which is more oriented towards military operations, the activities of ITAU would most likely be out of scope of the cyberwarfare. Yet, in principle, the fact that ITAU is a volunteer organization fighting on behalf of Ukraine, is conducting such operations that indeed match several of the cyberwarfare (or Cyber war) definitions (Clarke & Knake, 2011; Nicholson et al., 2012; Schaap, 2009). In this thesis, the term Cyberwarfare is understood as an activity of using cyber-capabilities to either *attack* hostile cyber-capabilities or *defend* friendly cyber-capabilities, where the actor can be a nation-state or a non-state actor.

However, the most typical tactic of ITAU is the denial-of-service attacks. As Svurudenko and Mozgin (2022, p. 41) articulate, a common method of attack in *hacktivism* is Denial of Service (DoS) and especially Distributed Denial of Service (DDoS). DoS attacks have the goal of disrupting information flow by subjecting a service – such as a website server – to a high number of requests and thus block authentic requests from being handled by the server. Traditionally DoS attack is defined as having a single source, such as an IP that it is sent from. Thus, an IP-based blocking can relatively easily mitigate such attacks. However, the distributed variant called DDoS attack relies on multiple sources to amplify its impact, and the sources can shift to make the mitigation efforts more challenging. They can also include multiple type of requests, and DDoS is often used via botnets, which can increase their impact exponentially.

While not usually included into the definition of Cyberwarfare, relevant to the activities of ITAU is also the information-domain (Hutchinson, 2001), including countering mis- and disinformation. Misinformation is usually defined as inaccurate or false information, that is deliberately created and propagated either intentionally or unintentionally (Jithesh, 2020; Wu et al., 2019). However, even if misinformation can be created and propagated intentionally, it is it's sibling the disinformation that is designed for deception purposes – meaning that disinformation is created and propagated to mislead others, as Starbird et al. (2019) argue. Ireton and Posetti (2018, p. 7) articulate disinformation as a deliberate and often orchestrated attempt to confuse or manipulate people by presenting dishonest information.

Information Warfare (IW) itself is a broad and sometimes an ambiguous concept, which has often been articulated to be an umbrella term under which literally all forms of warfare have been subjected to (Libicki, 2007, p.16). While relevant concept for this thesis, it is also important not to get tangled into too large of a conceptual quagmire of overlapping definitions. A quick recap of some of the most prevalent definitions of Information Warfare include several conceptualizations that differ somewhat in their emphasis. Dennig (1998) articulates that Information Warfare is at its core *operations that target or exploit information media in order to win some objective over an adversary* (p.1); while Hutchinson (2021) takes it over the precipice of information and writes in his Reappraisal of Information Warfare that it means *the use of data, information, and knowledge, and their associated technologies to manipulate information and the physical environment for the benefit of an attacker and against an opponent* (p.18). Hutchinsons (2021) appraisal is distinct from Dennings (1998) in that it distinguishes the difference of data, information, and knowledge – while defining them under *Information* Warfare – and explicitly stating that physical environment is a crucial part of it, while also defining it as the method of an *attacker*.

A seminal author on the matter, Martin Libicki, has also opened the term quite widely by first articulating that it involves *protection*, *manipulation*, *degradation*, and the *denial* of information in no less than seven domains: *command-and-control*; *intelligence*; *electronic warfare*; *psychological warfare*; *hacker warfare*; *economic information warfare*; and *cyberwarfare* (1995). Later (Libicki, 2007), also concluded that there needs to be some definition to use in reflecting these domains and coined the definition of Information Warfare to be *the use of information to attack information* (p.20) and use this to reflect into the different domains that were previously introduced, i.e., hacking a database to manipulate targeted information with false data. In this thesis, similar logic of using information to attack information is used when describing information warfare by the IT Army of Ukraine. However, while authors such as Libicki (1995; 2007) effectively label Cyberwarfare to be if not entirely, mostly, included inside Information Warfare, in this thesis the concept is used to cover actions that are less technically oriented but more about stealing, distributing, spreading information in order to influence their target by using information, i.e., massing fake Google reviews in order to spread information about the war-events in Ukraine - being also very close to the domain of Psychological warfare.

Psychological Warfare and Psychological Operations have often been used synonymously, and the preference of the former became due to the negative connotations perceived by the US public during the 1960's (Narula, 2004, p. 179). Psychological Operations (PSYOPS) can be well summarized in the definition of Narula (2004) as:

> "Planned use of all forms of communication/information and other psychological actions including political, military, economic and ideological actions, with the purpose of influencing the opinions, emotions, attitudes and behavior of hostile and non-hostile groups, both foreign and indigenous, in such a way as to support the achievement of national objectives." p. 187.

While Psychological warfare has its overlap with the other forms of warfare mentioned in previous paragraphs, it can be seen as having conceptual distinction with constructs such as Information Warfare. In this thesis, the concept of Psychological warfare and Psychological operations is understood with the definition of Narula (2004), with the heavy emphasis on influencing *emotions* of its target.

2.2 Cybergroups, hacktivism

In the cyber domain, there are a multitude of actors that can have a variety of roles in cyber conflicts (Schmitt, 2012) and cyber warfare (Clarke & Knaape, 2011; Shakarian et al., 2013). Some actors are individuals while some can be articulated to be cybergroups (i.e., implying a group that has some form of collective identity, purpose, and activity that is mediated by digital technologies and platforms). Sometimes the distinction between individuals and groups is not so clear, as in crowdsourced hacktivism (Johnson, 2014).

Hacktivism can be thought to be analogous to painting slogans to walls, disrupting services, and physical protests and its goal is usually to make a statement of support (or opposition) to a political or social cause (Webber & Yip, 2018). Common methods of hacktivists are website defacement and Distributed-Denial-of-Service attacks, which is a method of cyberattack that tries to stop the normal traffic of a target by sending large amounts of internet traffic to it, i.e., making legit connection to a website impossible (Deseriis, 2017). Some notable examples of this type of attacks, using crowdsourcing as a base, are done by the cybergroup Anonymous (Richards & Wood, 2018, p. 196) and the events that transpired during the Estonian cyberattacks in 2007 (Johnson, 2014, p. 6). Some authors such as Vegh (2002) have noted that the discourse of hacktivism after 9/11 attacks has changed, and which previously been termed hacktivism can now in some instances be labeled even as cyberterrorism.

Without going too deep into the definitions and research on terrorism, cyberterrorism is too an ambiguous term (Gordon & Ford, 2002), however, at its core the intent on producing destruction, violence, and severe harm to its target by (cyber)terrorists – being usually politically or ideologically motivated (Hua et al. 2018). The goal of their activity is often to promote fear in society, by having economic, societal, and psychological impacts (Gable, 2010; Gordon & Ford, 2002; Hua et al., 2018). What could be said to distinct cyberterrorist from cyber criminals, is that the terrorists focus on having a societal impact that usually is against states, while criminals have more financial incentives – however, both are articulated being unlawful activities (Gordon & Ford, 2002, p. 637).

Cybercriminals, as individuals or groups, engage in illegal activities in the cyber domain for various purposes, such as financial gain, information theft, or to create disruption; however, the boundary between cybercrime and traditional criminality is ambiguous and hazy at best (Anderson et al., 2013; Gordon & Ford, 2006). Cybercrime can in other terms be defined as traditional crimes perpetrated via cyber-means, and crimes that are characteristic of cyber technologies, e.g., hacking (Anderson et al., 2013). As one might conclude, acts per-formed as hacktivism can well be categorized as cybercrime, such as DDoS attacks.

There are two more concepts that have risen up fairly recently, *Cyberwarriors* (Ferretti et al., 2022) and *Cyber mercenaries* (da Cruz & Pedron, 2020; Maurer, 2018). Out of the two concepts, as da Cruz and Pedron (2020, p. 2) Cyber mercenaries seem to be the more ambiguous one, however they conclude that a cyber mercenary is much akin to the traditional mercenary, conducting (cyber)operations (usually illegally) for financial benefit (p. 3). Cyber mercenaries are also depicted as non-State actors, being more of an intermediary in the cyberwarfare domain (Maure). Cyber warriors on the other hand are articulated to be either military or civilian personnel of a state, and often divided between conducting offensive or defensive operations (Ferretti et al., 2022). Thus, one important differentiating aspect between the two terms is that while Cyber warriors are usually depicted as legitimate (often state-) actors, while Cyber mercenaries are seen as illegitimate and non-state actors.

The Tallinn Manual 2.0 gives quite solid foundations on the description of what a *non-State actor* is and what it is not in reflection to cyber operations; "*As a general rule, the cyber operations of private persons or groups are not attributable to States*" unless *"acting on the instructions of, or under the direction or control of, that State in carrying out the conduct"* further the manual states that:

> "…non-State actors include both individuals and groups. Groups are considered non-State actors under this Rule whether incorporated or unincorporated; hierarchical or non-hierarchical; organized or unorganized; and possessing domestic legal personality or not. The term encompasses, inter alia, individual hackers; informal groups like Anonymous; criminal organizations engaged in cybercrime; legal entities such as commercial IT services, software, and hardware companies; and cyber terrorists or insurgents." p. 95

Non-State actors thus encompass a very wide set of entities, which are notably differentiated from state actors (e.g., employed directly, or being a direct part of a government of a state). However, *state-sponsored actors* make this distinction more blurry, and while they are often not directly perceivable as a part of a state, they usually are backed by states resources and their activities orchestrated to at least some degree (Maurer, 2018). Also, the term state-sponsored in public language is often used due to attribution problems (Maurer, 2018, p. 23). In the literature, Advanced Persistent Threat (APT) actors are often articulated as the prime example of state-sponsored actors (Ahmad et al., 2019; Burita & Le, 2021; Lemay et al., 2018). While APT is often used as a term to describe a cyber-group (Lemay et al., 2018) that is well resourced, highly skilled, and very persistent and covert in their methodology. However, authors such as Ahmad et al. (2019) articulate that in the boarder literature APTs are refenced often as organized, malicious, and very sophisticated cyber campaigns. As clearly evident from the previous paragraphs and chapters, the Cyber-domain as a whole has conceptual complexity, and fittingly we next turn to Complexity Science itself.

2.3 Complex Adaptive Systems

Expanding on the notions of systems thinking (Merali & Allen, 2011), *complexity* is a concept that has been studied from a several perspectives (Cilliers & Spurrett, 1999; Levin, 1999). However, the term of complexity has no single, unified explanation – in fact, complexity, complexity theory, and complex adaptive systems have been used interchangeably in a wide range of studies (Preiser et al., 2018, p. 2). In similar line, there is a lack of unified theory of complexity (Thrift, 1999), which makes it reasonable to reflect the question that is there actually a solid discipline of complexity science – or do different scientific disciplines just have their own examples and issues of complex systems? (Ladyman et al., 1993).

The core of complexity theory centers around understanding and researching patterns of interaction between elements of a system, at different levels of analysis and time span, instead of individual elements that are isolated (McDaniel & Driebe, 2001). Complexity theory offers a multitude of concepts that can be applied and used alongside different theories to view complex phenomena in different ways, which can support transdisciplinary approaches (Gear et al., 2018; Ladyman et al., 1993). Some of the common concepts are agents, nonlinearity, feedback loops, coevolution, self-organization, emergence, boundaries, and complex adaptive systems. An *agent* represents an element of a system, which is capable of responding to other agents actions and information – these responses may be reactive but also learning and adaptation, where learning implicitly means that an agent has some type of memory of previous events (Cilliers, 1998, p. 92). In organizational terms, an element (e.g., agent) can be an individual, collective, or even a process of some type (Gear et al., 2018). An agent, especially in context of human organizations, is usually instilled with a schema, which is a cognitive structure that determines an agents actions in interacting with its environment (Anderson, 1999). These schemas are usually represented (and modelled) as a set of rules, that can be fuzzy and also evolve over time (Anderson, 1999, p. 219).

Nonlinearity is an essential concept in complexity science, since it is fundamental to the unpredictability of a system (Lewin, 1999, p. 11) – a property commonly attribute to a complex system (Richardson & Cilliers, 2001, p. 8). As a concept, nonlinearity can relatively simply be stated as a nonproportional output to inputs; i.e., having small inputs creating even unpredictably large outputs – such as in neural networks (Lewin, 1999, p.164). Nonlinearity can be articulated even as a precondition for other concepts of complexity to come about (Cilliers, 1998, p. 120), such as self-organization, emergence, and being far from equilibrium.

Feedback loops are a fundamental concept of complex systems, that either reinforce or negate change (Cilliers, 1998, p. 6); these feedback mechanisms can act in nonlinear ways (Anderson, 1999, p. 217) and be in a central role for the whole systems adaptation and evolution (Cilliers, 1998; Lewin, 1999, p. 189). Coevolution is in essence, mutual adaptation of agents based on each other interaction to one another, and also with the environment – such as in biological terms species not only evolve in respect to other species but that also their environment and ways of interaction evolve as well (Kauffman, 1996, pp. 113–114).

As in general (Schneider & Somers, 2006, p. 352) or simple (Roundy et al., 2018, p. 3) systems, *boundaries* are also essential in Complex Adaptive Systems (Holland, 2012, p. 51). Boundaries are needed to depict what constitutes the system, and said boundaries can be sharper or more ambiguous depending on what kind of a system and context is examined (Roundy et al., 2018, p. 3). Ambiguousness of boundaries can be an issue especially in complex systems, where the relationships and interactions between the components of a system is more important than depicting the strict boundaries of the system, and also that the agents in a complex system can have changing roles that transgress the boundaries of the system (Cilliers, 2001). This ambiguity is often due to the fact that complex systems, are often open systems (Pondy & Mitroff, 1979; von Bertalanffy, 1950). This openness is what enables the interaction with the system and its agents with its environment, exchanging information, energy, etc. and also enabling adaptation (Filotas et al., 2014). As Pondy and Mitroff (1979) argue, Open systems, especially in the organizational context, should not be viewed merely as subjects of influence from outside environment and having the ability to stay structured and coherent *despite* being open – but precisely having their structure and form because of them being inherently open to its environment.

Emergence is a phenomena, or behavior of a systems, which is not present or predictable based on individual components of a system (Holland, 2012, pp. 113–114). As an example, in complex adaptive systems such as organizations, emergence can be a novel way of conducting operations from interactions of organizational members – where a learned method can spread and transform the entire organization in a non-planned or managed way. Emergence is highly related to *self-organization* (Gear et al., 2018; von Bertalanffy, 1962, p. 15) and at its core is something that brings structure to the system in a spontaneous way, whether it is aspects such as relationships between agents or patterns of interaction between components and its environment (Cilliers, 1998, pp. 91–93). This is also highly connected to the ability of a system to adapt or coevolve, since these principles also require at least some type of "memory" in order to be possible; in order to self-organize, just as the global economy or an immune system self-organizes based on previous historical encounters and events.

However, despite the variety of terminology and principles – or because of it, the field of complexity science is prolific (Preiset et al. 2018; Richardson & Cilliers, 2001), and this has been especially the case in the domain of organizational studies (Lewin, 1999; Marion & Uhl-Bien, 2001; Richardson, 2008; Stacey, 1995; 1996) which intertwines with the topic of this thesis.

A distinct line in the Complexity theory, called *Complex Adaptive Systems theory* has also been used as a theoretical lens on a variety of studies, including organizational research (Boisot & Child, 1999; Carlisle & McMillan, 2006; Dooley, 1997; McDaniel et al., 2009; Schneider & Somers, 2006). Also, in previous related studies, CAS has been used to reflect *adversial attacks* (Behzadan & Munir, 2017), *Command & Control development* (Grisogono, 2006) as well as *Stuxnet-attack against Iran's nuclear facility* (Fekolkin, 2015). Marti (2018) has reflected *armies as CAS*, coming thematically to the thesis at hand. However, to use CAS as a theoretical lens, one must inevitably battle through the jungle of principles and features that the previous literature includes (Table 2).

Table 2 Principles/Feature of CAS found in literature.

Author(s)	Principles / Features
Holland, 1995	Aggregation, Nonlinearity, Flows, Diversity, Tagging, Internal models, Building blocks
Arthur et al. 1988; 1997	Dispersed interaction, No global controller, Cross-cutting hierarchical organization, Continual adaptation, Perpetual novelty, Out-of-equilibrium dynamics
Levin, 1998; 1999; 2005	Sustained diversity and individuality of components, Localized interactions among components, An autonomous process that selects from among those components, based on the results of local interactions
Cilliers, 1998	Large number of heterogenous components, Rich interaction of components, Nonlinear interaction, Abundance of feedback routes, No need for direct link for interaction of distant elements, Complex adaptive systems as open systems, Open systems operation under conditions far from equilibrium, Visually important system history, Subcomponents without access to all the information in the system.
Chu et al. 2003	Internal inhomogeneity of the system, Adaptivity of the agents in the system, Nonlinear interactions between parts of the system, Net-like causal structure of the system, Radical openness, Contextuality.
Buckley, 1968	Self-organization, Co-evolution, Feedback, Nonlinearity, Emergence, Diversity.
Preiset et al. 2018	Constituted relationally, Adaptive, Dynamic, Radically open, Contextual, Complex causality.
Lewin, 1999	Self-organization, Emergence, Feedback, Nonlinearity, Adaptation, Co-evolution
Anderson, 1999	Open systems, Nonlinearity, Adaptive, Self-organization, Co-evolution, Dynamic.

For this thesis, it was important to scan the most relevant literature and analyze what are the most important principles that have been used in example the organizational research. This part of the theoretical work was important for creating a suitable analytical lens, that would form the structure of the entire research and thesis. Relevant theoretical structures and concepts were aggregated and combined under descriptive principles that were recognized to represent the CAS in holistic and rigorous way. However, to use CAS as a practical analytical lens that did not spiral out of control by multitude of definitions, an aggregation of similar principles and features was conducted (Table 3).

Table 3 Aggregated CAS principles

CAS principle	Description
Adaptation/ Homeostasis	The ability of the system or its agents to adjust their behavior or structure in response to the changes in the environment or internal feedback (Holland, 1995; Levin, 1998; Chu et al. 2003; Buckley, 1968; Lewin, 1999; Anderson, 1999)
Nonlinearity	The property that small changes in inputs or parameters can lead to large and unpredictable changes in the outcome or output of the system (Holland, 1995; Arthur et al. 1988; Cilliers, 1998; Buckley, 1968; Lewin, 1999)
Emergence	The phenomenon that new patters, structures, or behaviors arise from the interactions of the agent without being explicitly planned or programmed (Buckley, 1968; Lewin, 1999).
Self-organization	The process by which order and coordination emerge from the local interactions of the agents without external control or direction (Holland, 1995; Cilliers, 1998; Buckley, 1968; Lewin, 1999)
Feedback	The mechanism by which information about the effects of actions or events is transmitted back to the source, influencing future actions or events (Holland, 1995; Levin, 1998; Buckley, 1968; Lewin, 1999)
Diversity/ Individuality	The variety and uniqueness of the agents and their attributes, which enable them to perform different roles and functions (Holland, 1995; Levin, 1999; Buckley, 1968; Preset et al. 2018)
Cooperation/ Communication	The degree and quality of interaction and collaboration among agents, which can enhance their collective performance and learning (Holland, 1995 (Tagging); Arthur et al. 1988 (Dispersed interaction); Cilliers, 1998 (Rich interaction of components)
Co-evolution	The process by which two or more systems influence each other's evolution through mutual adaptation (Arthur et al. 1988; Buckley, 1968; Anderson, 1999)
Openness/ Contextuality	The extent to which the system is influenced by and influences its environment, as well as its sensitivity to initial conditions and history (Cilliers, 1998; Chu et al. 2003; Preiset et al. 2018)

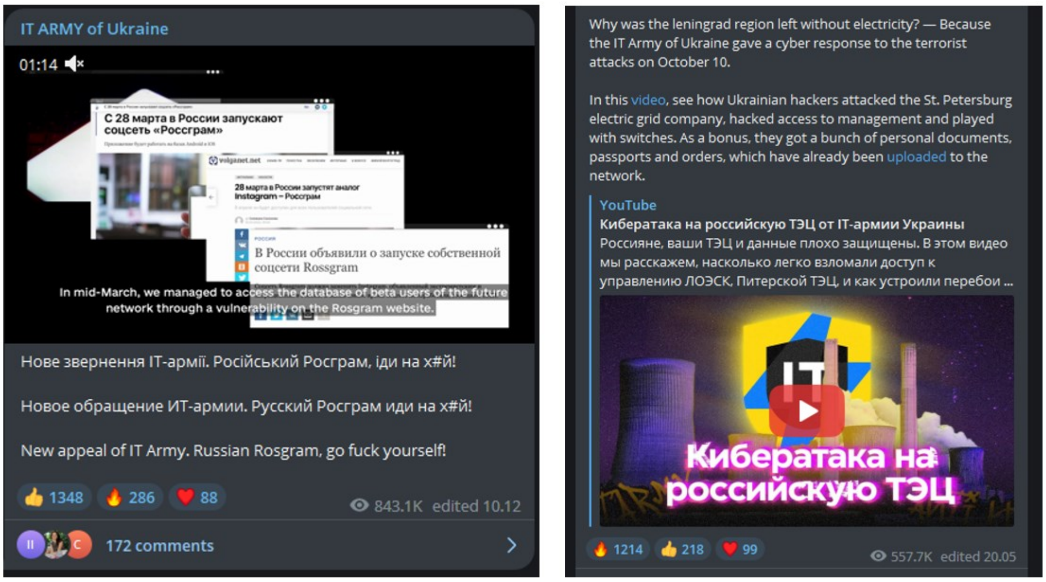
3 IT ARMY OF UKRAINE

The Ukrainian IT Army can be seen as having been born when the Ukrainian War escalated to its current full-scale war phase on February 24th, 2022. The official starting shot can be seen as having been two days later when the Ukrainian Minister of Digital Transformation, Mikhailo Fedorov, tweeted about the founding of the IT Army. In his tweet, Fedorov articulated that the battle would continue in the cyber-domain and called those that any skills in IT to join the fight. The creation of the ITAU was thus a spontaneous and ad-hoc, compared to some existing volunteer cyber-forces such as the EDL Cyber Unit (Estonian Defence League, 2023b) that enjoyed a more structured approach in their formation.

The phenomenon of cyber-groups forming *during* this war is not new in itself, and according to the observations made in the context of this paper, over 80 groups are taking active sides in the Russo-Ukrainian war – many of them created during the conflict. These groups are distributed relatively evenly between those with a pro-Ukraine and pro-Russia agenda. However, the IT Army of Ukraine (ITAU) in reflection to these other groups is distinct just by its mere size and the strong affiliation to the State of Ukraine. On a quick note, the ITAU could be articulated as being *state-sponsored hacktivist group* (Deseriis, 2017; Lucas, 2014; Svyrydenko & Mozgin, 2022), since its primary method of operation is using target listing in its Telegram channel to encourage crowdsourced Denial of Service (DoS/DDoS) attacks – which is a typical activity of hacktivist groups (Deseriis, 2017, p. 132). From the visible side, the ITAU is purely an offensive organization, which on the other hand distinguishes itself from more official counterparts such as the previously mentioned Cyber Unit of the Estonian Defence League (Estonian Defence League, 2023a).

However, there are indicators to higher capability of the group, that are more akin to APT-groups (Ahmad et al., 2019). Some of the first more sophisticated attacks that used the method usually known for hacktivists, included the defamations of the Sukhoi (GDC, 2022) and Gazprom (Reuters, 2022), the attacks were conducted in the first week of April, and reported by ITAU in their channel and YouTube on 23rd of April. Other notable operations were the attack to Rossgram, which is a Russian version on Instagram, and the attack on RuTube, which similarly is a Russian version of YouTube, and also the attack against a Electrical Grid Company in St. Petersburg. The Rossgram attack included the apparent breach of sign-up database, creation of a fake Rossgram-app, sending invites to those that used that had signed up for the app, and then revealing the hack via push notifications and leak the sign-up database to the public; as previously, the ITAU posted their attack in the form of a video in the ITAU Channel (Figure 1). The attack on RuTube-channels administration systems (Zotov, 2022) is also more sophisticated than mere DDoS, during the attack the administrators were physically isolated from the server rooms by wiping out their access rights – giving time for the attackers to hijack vital information and wipe the entire system database, showcased relatively high sophistication of capabilities.

Similar to the other more sophisticated operations of ITAU, the attack against a power grid company in St. Petersburg (Povaliaieva, 2022) was conducted entirely by the "invisible" part of the IT Army of Ukraine. There were no prior discussion about the attacks, or mentions of them, until the attacks were public. However, the ITAU has made sure to put an effort into promoting their results (Figure 1) in YouTube and their channel.


IT ARMY of Ukraine
01:14
С 28 марта в России запускают соцсеть «Россграм»
volganet.net
28 марта в России запустят аналог Instagram – Росграм
РОССИЯ
В России объявили о запуске собственной соцсети Rossgram
👍 1348
🔥 286
❤ 88
843.1K edited 10.12
172 comments
YouTube
Кибератака на российскую ТЭЦ
🔥 1214
👍 218
❤ 99
557.7K edited 20.05

In mid-March, we managed to access the database of beta users of the future network through a vulnerability on the Rosgram website.

Нове звернення IT-армії. Російський Росграм, іди на х#й!

Новое обращение ИТ-армии. Русский Рсграм иди на х#й!

New appeal of IT Army. Russian Rosgram, go fuck yourself!

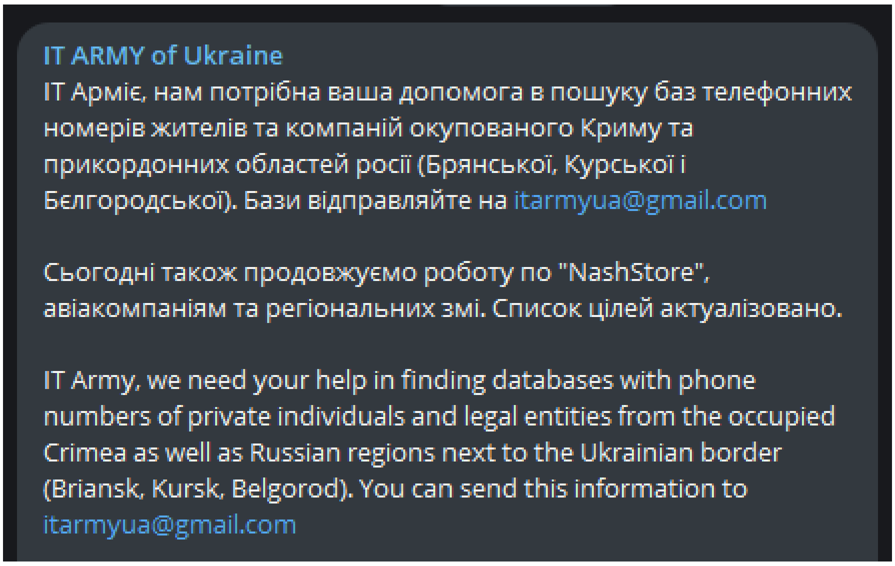
Why was the leningrad region left without electricity? — Because the IT Army of Ukraine gave a cyber response to the terrorist attacks on October 10.

In this video, see how Ukrainian hackers attacked the St. Petersburg electric grid company, hacked access to management and played with switches. As a bonus, they got a bunch of personal documents, passports and orders, which have already been uploaded to the network.

Кибератака на российскую ТЭЦ от IT-армии Украины
Россияне, ваши ТЭЦ и данные плохо защищены. В этом видео мы расскажем, насколько легко взломали доступ к управлению ЛОЭСК, Питерской ТЭЦ, и как устроили перебои ...

Figure 1 Attacks on Rosgram and St. Petersburg EGC in ITAU Channel

The ITAU can also be seen operating in three different (warfare)dimensions; psychological (Wallenius, 2022, p. 24), information (Hutchinson, 2021; Hutchinson & Warren, 2001). ITAU has repeatedly posted calls for databases and information leaks (as in example Figure 2), as well as propagating and using hacked and leaked databases and information (as in Figure 3).



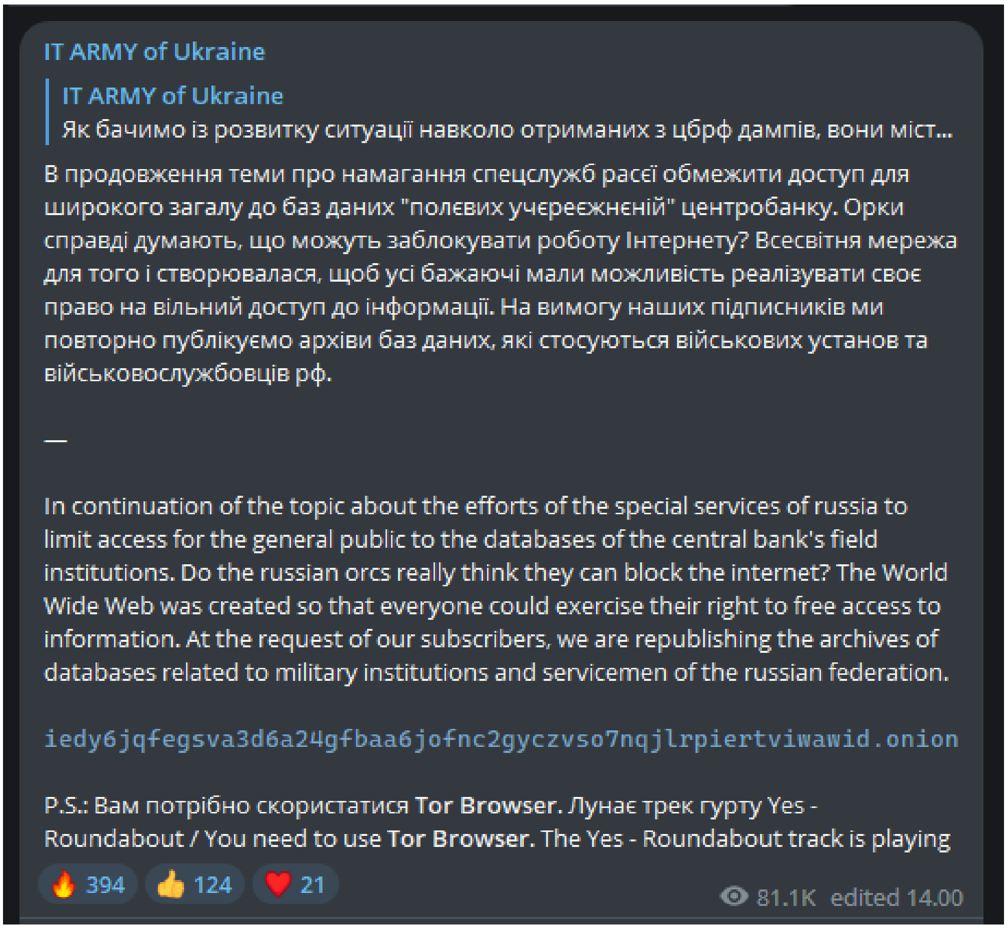
IT ARMY of Ukraine

IT Арміє, нам потрібна ваша допомога в пошуку баз телефонних номерів жителів та компаній окупованого Криму та прикордонних областей росії (Брянської, Курської і Бєлгородської). Бази відправляйте на itarmyua@gmail.com

Сьогодні також продовжуємо роботу по "NashStore", авіакомпаніям та регіональних змі. Список цілей актуалізовано.

IT Army, we need your help in finding databases with phone numbers of private individuals and legal entities from the occupied Crimea as well as Russian regions next to the Ukrainian border (Briansk, Kursk, Belgorod). You can send this information to itarmyua@gmail.com

Figure 2 Call for crowdsourced information and databases.



IT ARMY of Ukraine

> IT ARMY of Ukraine
> Як бачимо із розвитку ситуації навколо отриманих з цбрф дампів, вони міст...

В продовження теми про намагання спецслужб расеї обмежити доступ для широкого загалу до баз даних "полєвих учєреєжнєній" центробанку. Орки справді думають, що можуть заблокувати роботу Інтернету? Всесвітня мережа для того і створювалася, щоб усі бажаючі мали можливість реалізувати своє право на вільний доступ до інформації. На вимогу наших підписників ми повторно публікуємо архіви баз даних, які стосуються військових установ та військовослужбовців рф.

—

In continuation of the topic about the efforts of the special services of russia to limit access for the general public to the databases of the central bank's field institutions. Do the russian orcs really think they can block the internet? The World Wide Web was created so that everyone could exercise their right to free access to information. At the request of our subscribers, we are republishing the archives of databases related to military institutions and servicemen of the russian federation.

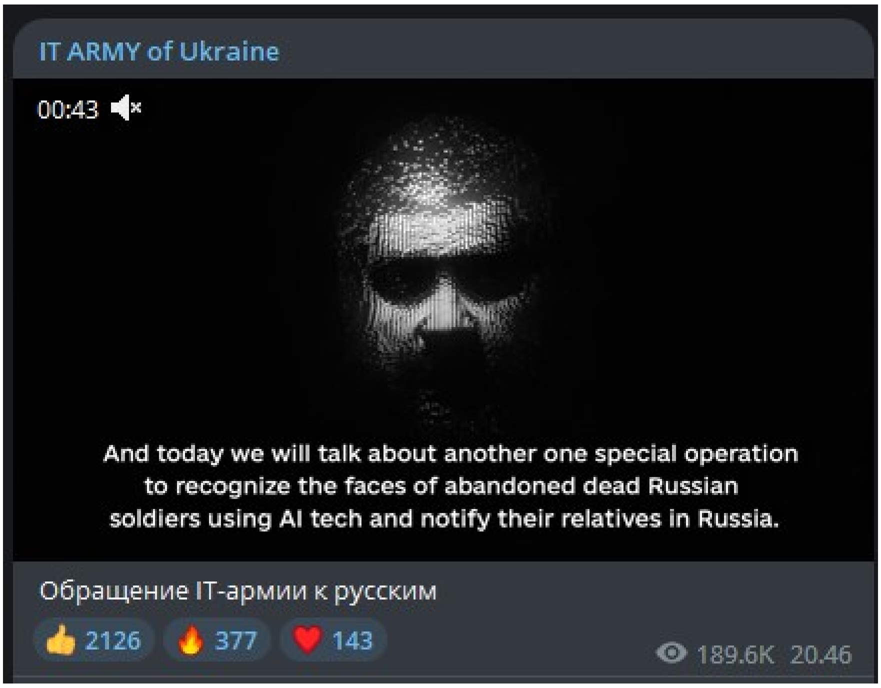
`iedy6jqfegsva3d6a24gfbaa6jofnc2gyczvso7nqjlrpiertviwawid.onion`

P.S.: Вам потрібно скористатися **Tor Browser**. Лунає трек гурту Yes - Roundabout / You need to use **Tor Browser**. The Yes - Roundabout track is playing

🔥 394 👍 124 ❤ 21 👁 81.1K edited 14.00

Figure 3 ITAU propagating leaked databases

The operations in the Information warfare-domain often overlap with the psychological aspects, and a notable example is the usage of Clearview AI for facial recognition of dead Russian soldiers (Dave & Dastin, 2022) and calling the relatives of the deceased to inform them about it (Figure 4). The ITAU also have used similar tactic of calling relatives[1] of Russian soldiers that have been seemingly looting in Ukraine and sending looted materials to Russia by recognizing Russian soldiers from CCTV footage. These operations, such as one described in Figure 5, require skills and resources that go beyond the casual DDoS attacks and are possibly conducted in cooperation with Ukrainian intelligence or military organizations.



And today we will talk about another one special operation to recognize the faces of abandoned dead Russian soldiers using AI tech and notify their relatives in Russia.

Обращение IT-армии к русским

Figure 4 ITAU Info/Psyops by calling the relatives of Russian casualties.

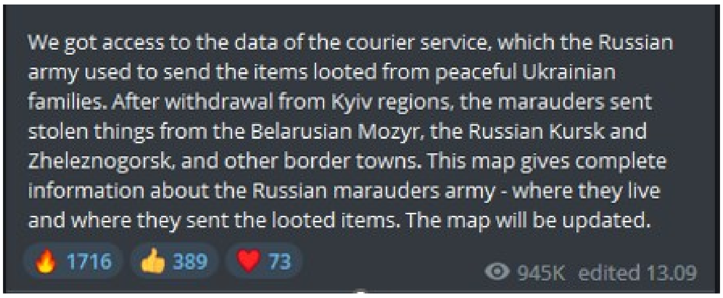
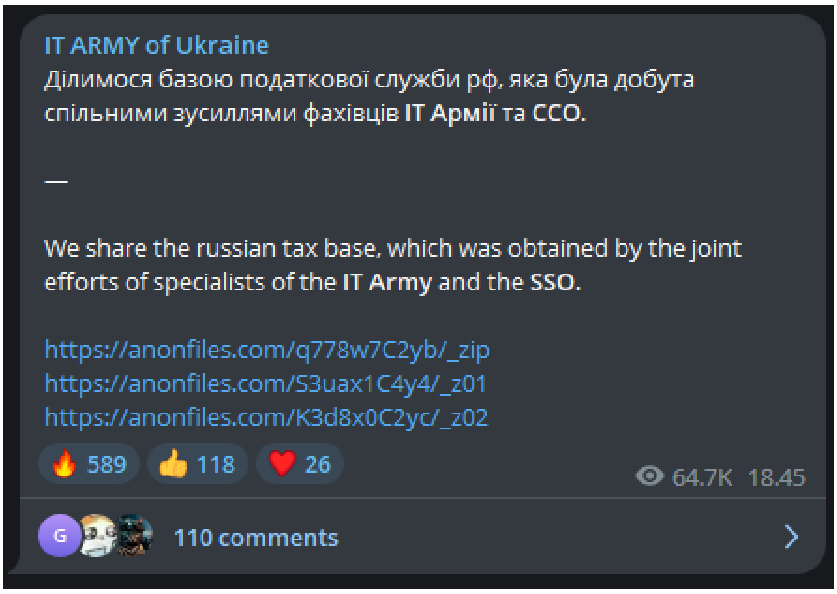

We got access to the data of the courier service, which the Russian army used to send the items looted from peaceful Ukrainian families. After withdrawal from Kyiv regions, the marauders sent stolen things from the Belarusian Mozyr, the Russian Kursk and Zheleznogorsk, and other border towns. This map gives complete information about the Russian marauders army - where they live and where they sent the looted items. The map will be updated.

Figure 5 Sharing location data of courier service used by Russian looters

[1] Example of phone call with relatives of looters by ITAU: https://www.youtube.com/watch?v=yvH_TLXS4oY

These actions that require more skills and capability, such as making the phone calls to relatives of Russian soldiers, are more related to the "invisible" side of the ITAU – a non-crowdsourced activity. These operations are also often combinations of hacking sources and then leveraging leaked information for propagation to counter targets such as the Russian narrative of having little losses in the "special military operation" or publicly shaming participants and creating psychological pressures to other stakeholders such as soldiers relatives. As previously mentioned, cooperation with other Ukrainian organizations is something that occasionally the ITAU explicitly state themselves, as seen in a post on 13th of October 2022 (Figure 6).



IT ARMY of Ukraine

Ділимося базою податкової служби рф, яка була добута спільними зусиллями фахівців **IT Армії** та **ССО.**

—

We share the russian tax base, which was obtained by the joint efforts of specialists of the **IT Army** and the **SSO.**

https://anonfiles.com/q778w7C2yb/_zip
https://anonfiles.com/S3uax1C4y4/_z01
https://anonfiles.com/K3d8x0C2yc/_z02

🔥 589 👍 118 ❤️ 26 64.7K 18.45

110 comments

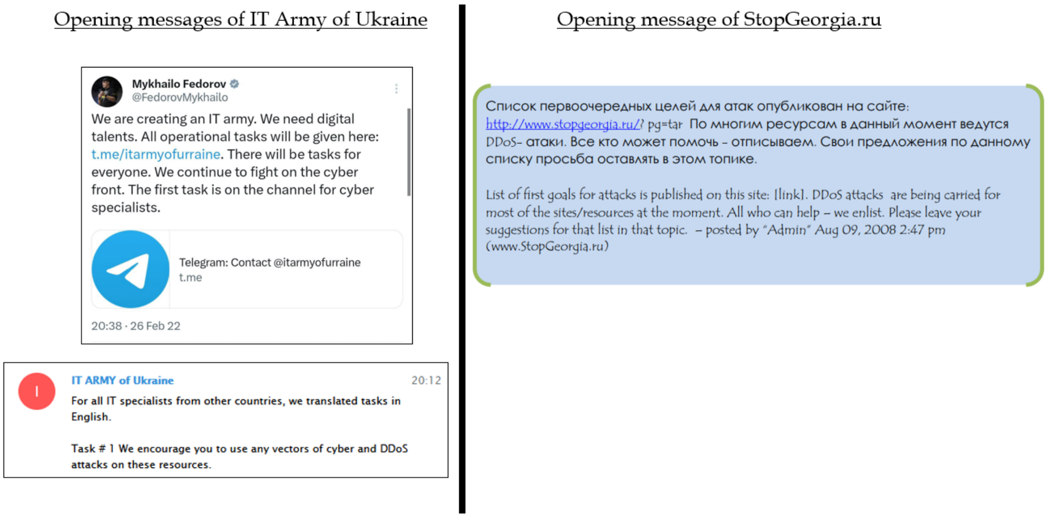
Figure 6 Leaking tax base from a joint operation with the SSO [2].

While attribution is often "in plain sight" with ITAU, the difficulty of attribution is usually typical in the cyber-domain (Robinson et al., 2018, p. 75) and additional challenge to attribution comes through the activity of hacktivists (Johnson, 2014, p. 5). The use of social media in hacktivism and in other cyber-operations has been described as making attribution more difficult (Johnson, 2014, p. 2) and an example of this type of an attack, Johnson (2014, p. 6) has described the Estonia cyberattacks in 2007 as one of the first *crowdsourced* cyberattacks. Quite similarly to the Estonian incidents, the ITAU's logic of action is succinctly to create continuous disruption within Russian society, particularly by complicating the use of all cyber resources related to Russia or its operation. However, instead of focusing only on single event or target such as a date or specific government sites, they pursue a wide and continuous avenue of operations.

While the IT Army of Ukraine emerges as a phenomenon that stands out both in size and its closeness to state affiliation and attribution, there is especial-

[2] The Ukrainian Special Service Operations: https://sof.mil.gov.ua/

ly one among several cyber conflicts (McReynolds, 2015) that strikes similar resemblance. This occurred during the 2008 Georgian-Russian conflict, where DDoS attacks coincided with Russian troop movements into South Ossetia (Korns & Kastenberg, 2008). The Georgian-Russian cyber conflict was investigated by Project Grey Goose[3], which was on organization composed of over 100 volunteers in the US security industry. Much like the ITAU, the crowdsourced side of the operation was coordinated through a website, where methods, techniques, and targets were listed. The site was however restricted from certain IP-ranges when it was apparent that there were investigators examining it – contrary to the ITAU, which has had its channels open despite of pro-Russian efforts of disrupting it. The most describing fact between these two organizations can be perceived through the first messages that initiated their activities (Figure 7).



Opening messages of IT Army of Ukraine

Mykhailo Fedorov
@FedorovMykhailo
We are creating an IT army. We need digital talents. All operational tasks will be given here: t.me/itarmyofurraine. There will be tasks for everyone. We continue to fight on the cyber front. The first task is on the channel for cyber specialists.

Telegram: Contact @itarmyofurraine
t.me

20:38 · 26 Feb 22

IT ARMY of Ukraine 20:12
For all IT specialists from other countries, we translated tasks in English.

Task # 1 We encourage you to use any vectors of cyber and DDoS attacks on these resources.

Opening message of StopGeorgia.ru

Список первоочередных целей для атак опубликован на сайте: http://www.stopgeorgia.ru/? pg=tar По многим ресурсам в данный момент ведутся DDoS- атаки. Все кто может помочь - отписываем. Свои предложения по данному списку просьба оставлять в этом топике.

List of first goals for attacks is published on this site: [link]. DDoS attacks are being carried for most of the sites/resources at the moment. All who can help – we enlist. Please leave your suggestions for that list in that topic. – posted by "Admin" Aug 09, 2008 2:47 pm (www.StopGeorgia.ru)

Figure 7 Starting messages of ITAU and StopGeorgia

In the previous Figure 7, the opening messages of the ITAU are from the Minister of Digital Transformation, who calls for digital talents to fight for Ukraine and points towards the coordinating hub – the Telegram channel. Roughly at the same time, the Telegram channel of ITAU had their first message and encouraged to use any vectors of cyber and DDoS attacks on the resources of the first target list. In quite similar fashion, in 2008 the "Admin" of the website and forum of StopGeorgia posted a message calling for anyone who can help and pointed also to the coordinating hub for attacks (webpage-link), while articulating that DDoS attacks are already on their way on many of the targets that they have presented and encouraging for more targets.

[3] Project Grey Goose: http://static1.1.sqspcdn.com/static/f/956646/23364659/1377188846503/Project-Grey-Goose-Phase-I-Report+on+Georgia.pdf

In the case of Grey Goose, it was difficult to prove direct state attribution, although there seemed to be coordination between cyber-attacks and military operations (Harrison Dinniss, 2012, p. 290). As said, StopGeorgia had their activities very much synchronized with the military actions of the Russian Federation on the Georgian war (Korns & Kastenberg, 2008). Similarly, the ITAU has been very reactive to the events happening in the environment, or more precisely in relation to the war and the two countries in the middle of it, Ukraine and Russia. This responsiveness becomes visible mostly through the public channels, where for example targets are listed in relation to events happening "on the ground" – such as targeting MacDonalds for its slow response of leaving the Russian markets. This largely represents reaction to the information that is received through media and social media channels, which resemble the kind of socio-political responsiveness that groups such as the Anonymous has in its campaign against ISIS (Richards & Wood, 2018).

It also has resemblance to the other Anonymous operations, such as "Operation Payback" against institutions and individuals that they perceived as being instrumental in censoring Wikileaks (McReynolds, 2015, p.427). Methods of attack were also primarily DDoS by using the Low Orbit Ion Cannon (or LOIC), which enabled central control of personal computers to send requests to targeted servers (p.427). The speed of operations – tempo – is in the ITAU much faster, creating similar operations often on a daily basis. Tempo being one aspect that differentiates ITAU from previous hacktivist campaigns, it also has other characteristics that make it complex, as well as *adaptive*. And due to this, we turn our theoretical lens towards the concepts found in the burgeoning field of complexity science and our methodology to virtual ethnography-orientation, in order to bring insights into the dynamics of the group.

4 METHODOLOGY

In this study, the research goal is to gain deep understanding of the properties of the IT Army of Ukraine, using CAS as a theoretical lens. CAS includes principles such as adaptation, nonlinearity, emergence, self-organization, feedback, diversity, and co-evolution (Buckley, 1968; Cilliers, 1998; Levin, 1999; Lewin, 1999). In order to achieve rich enough understanding of the ITAU, the research in this thesis is best articulated as *ethnography-oriented case study*. As Yin (2018) writes, a case study research comprises all-encompassing mode of inquiry (p.46), that investigates a contemporary phenomenon it its real-world context (p.45). However, as noticed on the preliminary observations, the systemic workings of ITAU have such socio-cultural aspects that ethnography-oriented research approach was seen necessary. It is also increasingly argued, that combined methodological settings is needed in complex organizational settings – such as *organizational ethnographic case studies* (Côté-Boileau et al., 2020).

This kind of approach can lead to challenges in utilizing the mass of data that is accrued through the study, and lead to research paralysis through overwhelming (Côté-Boileau et al. 2020, p.11). Using sensible scoping in the gathering of data, and doing pragmatic combination of methods (Flick, 2018a), can enable the strengths of triangulation of data (Côté-Boileau et al., 2020, p. 11; Flick, 2018b) while steering away from overwhelming the researcher. As an example, it was decided that the methods such as semi-structured interviews were scoped out of the study, as were other active and interactive methods towards the members of the community – by purely research practical and also ethical reasons (Driscoll & Gregg, 2010).

Quantitative methods have been dominant in general CAS studies outside of organizational studies. However, qualitative methods have been articulated as being very suitable for the study of complex systems due to their richness of data and flexibility of research process (Roundy et al. 2018). The researcher's ability to capture evidence that illustrates the fundamental concepts of a theoretical perspective, determines the usefulness of that perspective for understanding the phenomena in question. Ethnography has been previously argued to be a significant methodology – more than just a single method – to study

CAS especially from social and organizational contexts (Güney, 2010, p.274). However, the context of this study situated practically completely in a technology-mediated, digital domain, a more specific form of ethnography-orientation needed to be in place.

4.1 Ethnography in the digital/virtual domain

Central part of ethnographic research is the focus of studying the activity of people in their natural environment, where the role of the researcher is usually either an active participant or a passive observer (Brewer, 2000, p. 10). At times ethnography is articulated to be a holistic methodology of qualitative research, and at time it is understood more as a way of gathering data. However, irrespective of the understanding of the breath of ethnography, what is common is the extensive fieldwork that can last from several months to years (Brewer, 2000, p. 45; Güney, 2010, p. 281), which is also the case in this study, with a full 12 moths of research. Since ITAU at its core is crowdsourced activity coordinated through social media platform Telegram, having a research methodology that has a long track record of being applied to the study of online communities (Kozinets, 2010) was deemed appropriate. This made sense also from the perspective of CAS, since several principles that make the theoretical underpinnings of CAS rely on the aspect of social interaction and livid communication of the members of ITAU.

Ethnography itself in the online, or cyberspace, has its own methodological perspectives as well as proposals on how to approach them (Domíniquez et al., 2007). The same ambiguity and variety are apparent in the terminology of the field, depending often on slight variations of approach in studies. Kozinets (2010) uses the term "*online ethnography*", to describe ethnographic study in the context studying communities in cyberspace. He goes further to describe "*Netnography*" (2010, p.4) as a way of conducting research where the source of data comes from computer mediated interaction and which has the aim to produce understanding of cultural or communal phenomena – utilizing blogs, forums, social networking sites, and imageboards (2010, p.1).

Some authors such as Fields and Kafai (2009) as well as Hine (2007) have used the term "*connective ethnography*" to describe their approach, which utilized a variety of data sources both online and offline to understand their researched context and to avoid strict divisions between online and offline environments.

In similar fashion, Murthy (2008) as well as Wesch (2009) articulate "*digital ethnography*" to be focused on researching digital content such as videos, social networking sites as well as blogs/vlogs, with the aim of harness several methods and data sources to gain a balanced understanding of the researched subject. However, when describing the role of the researcher, Murthy (2008, p. 840) articulates that often in the digital domain the researcher is a "lurker" and depending on the proper approach to the context might be completely passive.

This role of being solely an "outside observer" is also at the core of "*webnography*", that focuses mostly on websites such as discussion boards and blogs (Puri, 2007).

While *digital ethnography* and *webnography* reserves the option to be a purely in the digital realm, "*cyber ethnography*" as articulated by authors such as Ward (1999) and Rybas and Gajjala (2007), focus exactly on the technological junctures where the digital and the "real" worlds overlap – not necessarily meaning digital and physical worlds but that communication via email or discussions in a chat-rooms are just as "real" as communication face-to-face. As Ward (1999, p.2) articulates, "*physical and virtual realms are becoming increasingly difficult to separate…*" and that from the two a new, hybrid space emerges. In "*Virtual ethnography*" Hine (2000) articulates in a similar fashion that computer-mediated communication in fact creates a space for community formation. Hine (2000) sees that technology – such as the internet - produces social structures that overextend the notions of simple online/offline categorization. In virtual ethnography, the study context is shaped by the interaction between people and the technology that is used; which makes also the role and position of the researcher very critical in reflexivity (Hine, 2000, p.48; 54).

4.2 Research ethics

Research ethics, especially in the methodology of ethnography in online settings, can be a challenging concept to handle. Research in online context can include retrieving data from a variety of websites, and which can include communal sites such as blogs, forums, chatrooms, social networking and media sites. What usually differentiates these sources from other research data such as interviews, is that they are not explicitly made for research purposes (Sugiura et al., 2017). Due to this, considering the basic principles of research ethics such as anonymity, informed consent, and privacy should be treated with highlighted focus and reflection.

Informed consent. The core of this research is conducted in the Telegram-platform and includes a channel and a chatgroup. Both of these entities are fundamentally open in nature, and do not require invitations or registering to join. Telegram, and Telegram-channels are known to be used for both private and public purposes; channels and groups are used to purposes such as conveying information to larger audiences, while closed groups and 1-on-1 instant messaging can be entirely private in nature. Posts in notable Telegram-channels are also known to be sometimes highlighted in media outlets and other social media platforms such as Twitter, Instagram, or Facebook.

Why this matters is that it is paramount to gain understanding of how the members of the group possibly *perceive the privacy of their contributions* – a researcher should not make the assumption that if the community is open to the world, that the members of the group would not have the experience of being in a closed and private environment (Frankel & Siang, 1999). Considering whether the group is open or not, makes a difference especially on considerations on informed consent. The literature and ethical guidelines are often inconclusive, sometimes ambiguous, and even conflicting on the matter. Notable authors on the subject such as Kozinets (2002, 2010) articulate that despite how open or closed a community is, a researcher should always fully disclose themselves. Langer and Beckman (2005) articulate the opposite; they find that the approach Kozinets (2002) takes is too constrictive and severely limit the ability of the researcher to conduct research. In fact, as Sugiura et al. (2017) came to notice, that seeking consent and even informing the presence of the researcher in a discussion forum can prove to have significant negative consequences such as abusive comments, avoidance of posting, moderating the researchers posts away etc. (p. 190) and eventually they decided to continue the research as "lurkers". Further question can be raised up on what protective practices can be done to protect the researchers, if following strict ethical considerations can paint the researcher as a target for online harassment?

Informed consent in online community contexts can be achieved via direct approach to distinct members of the group, which can prove to be unpractical especially in larger communities and can even be considered spamming (Hewson, 2003, p. 82). Contacting the moderators of the group can also be one way to approach, however moderators cannot give consent on behalf of the members (Sugiura et al., 2017, p. 192). Common method of creating transparency and give options for consent is posting an informative message, which should be done iteratively and extensively to gain maximum reach; however, this approach can give issues that were mentioned in the previous paragraph.

Pursuing ethnographic research without informed consent and being a passive observant is in online ethnographic research articulated as "lurking" (Hine, 2000). As a "lurker", the researcher is both covert and passive, using "cyber stealth" (Ebo, 1998). This approach has been used repeatedly in previous literature (Björk & Kauppinen-Räisänen, 2012; Hine, 2000; Mkono, 2011). One motivation to utilize "lurking" is to perceive the natural context of interaction and activity, since the activity of the researcher can significantly influence the domain (Hine, 2000).

Conducting research in "stealth mode" and especially in context of groups that are harder to reach, such as people conducting piratism (Cooper & Harrison, 2001) or identity theft (Holt & Lampke, 2010) gives added weight for anonymity and privacy of the researched subject(s). Also, in online-contexts the ability to re-track text strings through search engines has to be taken into consideration – pseudonymization does not work if the sentence can be found via search sentence. Practices such as summarizing data and re-writing possible quotes in order to reduce the possibility of discovery (Sugiura et al., 2017) can be used to mitigate the effects of text-based search engines. As a conclusion, while utilizing strict ethical and privacy-protecting protocols can prove challenging from the perspective of the researcher, it was seen extremely essential for this context, and thus effort was made to achieve rigor during the entire research.

4.3 Procedure

Virtual ethnography-orientation (Hine, 2000) was selected as a partner in research methodology, due to the nature of the researched subject. Virtual ethnography takes the perspective that instead of studying a community as in ethnography, the study examines what actually represents a community, its boundaries and perhaps even several communities (Ward, 1999).

Virtual ethnography was also selected as a method, because the researcher had previous experience in using the methodology (Merilehto, 2022; Merilehto & Riihikoski, 2022). This experience and methodological knowledge aided in reflexivity (Levitt et al., 2018) during the procedure of the study. Also, understanding of the context-related language (Hutchins & Klausen, 1996, p. 5) brought additional fluency and rigor to the procedure an analysis of the study, since the researcher had extensive knowledge of the vocabulary and terminology used in the researched context (i.e., hacking, information technology, information warfare).

The ethnography-oriented study in this thesis mainly constituted the examination of Telegram channel "IT Army of Ukraine" and its related chat group. In addition to that, news outlets, social media, and the ITAU website were consistently monitored to triangulate events and to gain insights into the ITAU composition and operations. Major part of the communication in both the channel and the chat, especially by the participants, was conducted in Ukrainian language. This represented a challenge for the researcher, who while being fluent in English, did not have background in Ukrainian or Russian. However, when using mobile phone as the user interface, it was possible to use the integrated translation in Telegram and while using the Desktop-application, it was possible to use other available translator to copy-paste text, such as Google Translator. To make the process of recognizing content, the researcher however made an effort to learn the Cyrillic alphabet to quickly recognize entities such as locations, companies, and tools.

After extensive ethical considerations, the scope of the gathering of material during the study, it was decided that the anonymity of and privacy of the participants in the channel should have enhanced priority. This was especially since it was also noted that applying the principles of informed consent before the study proved to be a significant challenge for the researched context (see section 4.2 on ethics). Thus, the material gathered from the IT Army of Ukraine Telegram channel and chat consisted of field-notes, such as re-written excerpts from posts of participants, screenshots of the ITAU Bot and Channel Admin, and screenshots of items where there were no or extremely unlikely to recognize the poster.

Quantitative data, such as the changes in the number of users were retrieved from services such as TGStat or through the Telegram API. During the research, the standard operating procedure was to exclude saving any items that incorporated personal information or information where personal information could easily be assumed to be extrapolated or interpreted from such as Telegram usernames. Text excerpts were rewritten in order to mitigate the possibility of using in-application search function to easily search for the posters of specific messages. However, the messages posted by the Bot and the Channel admin did not enjoy this privilege, since at the time of writing, chat-bots did not enjoy privacy rights similar to natural persons. Also, since both ITAU Channel and Chat are open groups, it was interpreted with relative confidence that the Admins of ITAU intended their messages to be publicly available.

The empirical data and other research materials were stored in the hosted server of the University of Jyväskylä, while analysis and processing of the material was done in the Office365 environment provided by the University of Jyväskylä. Both practices followed the guidelines of the University, in both storing and processing the data – especially since no personal data was collected or processed. The procedure of the study also followed general ethical guidelines of the University and General Data Protection Regulation (GDPR). Other research ethical guidelines and frameworks that were consulted included the products of the Association of Internet Researchers (AoIR), the British Psychological Society (BPS), the British Educational Research Association (BERA), the Council of American Survey Research Organizations (CASRO), the Market Research Association and the Association of Social Anthropologist of the UK and Commonwealth (AASA).

The study of the ITAU Channel and Chat included regular daily checks on new posts, longer observation-sessions (for up to 3 hours) where the Channel and Chat were intensely monitored, and retrospective reading of older posts. In the first months of the study, especially the longer monitoring sessions combined with longer retrospective analysis proved to be necessary since the amount of messages especially in the Chat were quickly overwhelming, and could in a matter of hours be several hundreds of messages – majority in Ukrainian language. The official empirical portion – virtual ethnography – of the study lasted for 15 months from February 2022 to May 2023. Analysis of the gathered material was continuous, while during the latter parts of the study the weight of data gathering versus analysis shifted towards forming the core of the findings due to the saturation effect. However, the presence of the analytical lens was present from the beginning, and acted as a guiding lens for the data gathering efforts. This did not mean that finding data to forcibly fit into certain was driving the efforts, but more as a way of structuring findings. This resulted in the emphasis on certain principles, which was expected. Since gathered data mostly consisted on field notes and screenshots, the list of different sources in the data source table (Table 4) is short. The overall procedure is also depicted in Figure 8.

Table 4 Data source table

Data source table	Pages (Font 11, 1-line)
Field notes	76
Screenshots	203

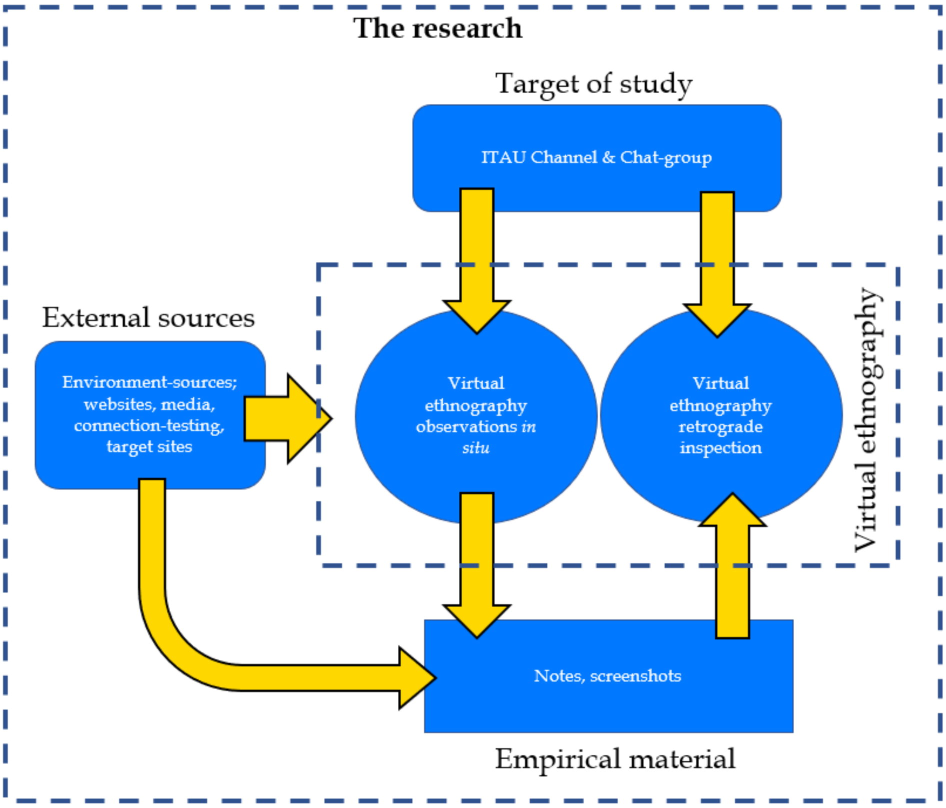

The research
Target of study
ITAU Channel & Chat-group
External sources
Environment-sources; websites, media, connection-testing, target sites
Virtual ethnography observations *in situ*
Virtual ethnography retrograde inspection
Virtual ethnography
Notes, screenshots
Empirical material

Figure 8 The overall procedure of the study

4.4 A note on the methodological rigor of the research

Tackling challenges of validity, and reliability in research is best to be done as early as possible (Levitt et al., 2018). In qualitative studies, which this thesis represents, the terms validity and reliability are sometimes replaced with the terms *credibility*, *transferability*, *dependability*, and *confirmability* – especially in the case of the constructivist paradigm (Denzin & Lincoln, 2017, p. 57). In this thesis, the term validity is meant to represent the accuracy, truthfulness, and credibility of the findings, meaning the extent to which the study represents the phenomena its intended to reflect (Creswell & Miller, 2000). Reliability, on the other hand, is understood in this thesis as consistency in research methodology, i.e., whether the research would yield similar results if replicated in the same context (Golafshani, 2003). As previously mentioned, often these terms are substituted to a language that reflects more the work of qualitative than quantitative research, they are used in this thesis. However, the more descriptive terminology is also used where necessary to enrich descriptions.

When the topic of this research first became relevant, the possibility was discussed immediately on an idea-level with practitioners in the field of cyber security and information security, as well as with the researchers own network of PhD students. The topic was further introduced to an assistant professor who had previous experience in ethnography and was familiar with the researcher's previous work. Based on the input from these external sources, a methodological structure was formed and aligned with the possibilities of data gathering techniques from the ITAU channel.

Diverse discussions with PhD researcher of complexity science affirmed the theoretical lens that was to be used in this study, which is the Complex Adaptive Systems (Cilliers, 1998; Levin, 2002). The researcher being already familiar with another contextually close (Gureckis & Goldstone, 2006) theoretical lens, the Distributed Cognition (Hollan et al., 2000; Hutchins, 1995), the relevant theoretical structures were quickly recognized and internalized after preliminary literature review on the subject. Armed with a suitable theoretical lens and robust methodological perspective, the researched context could be studied with good rigor from the early start.

While having a clear continuum as a process, the research in this thesis can be best summarized to be iterative in the form of a hermeneutic circle, where theory and empirical aspects influenced each other in a continuous manner (Puusa & Juuti, 2020). The empirical portion of the study can be said to have formed its own "triangulative circle" by triangulating data (Flick, 2018, p.4) from the on-going and in-situ virtual ethnography, the notes and findings archived from it and the archive of ITAU channel and chat-group, and the supporting material such as media outlets and observations from targeted sites. On the theoretical side, the used theoretical frame (CAS), the background literature on it and the subject matter (in example, Cyber warfare etc.), and the research questions "discussed" together to form a solid understanding of the theoretical scope. In a broader manner, the theory guided the structuring of empirical findings, while the empirical data gave input to further consolidate the theoretical lens and re-affirm what insights could be gained from the researched topic. Concordance with the findings and existing literature brings certainty to the findings of the study (Morse, 2017, p. 1392). This overview of the methodological circle can be found in Figure 9.

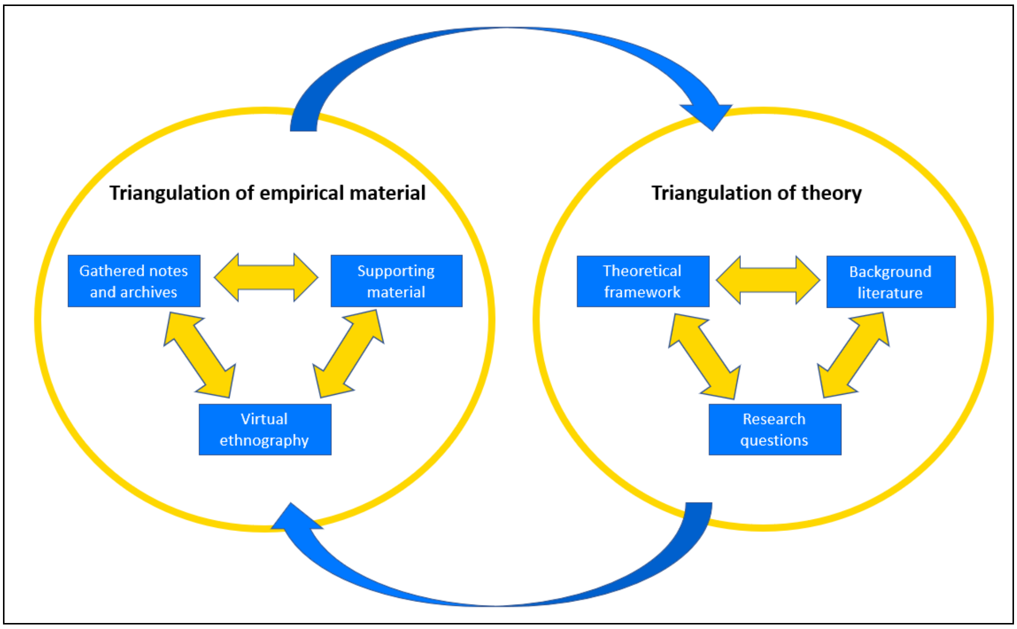


Figure 9 Overview of research

One method of gaining consistency in results (Levitt et al., 2018) was to always have multiple and repeatable cases of patterns of behavior, in example when articulating the phenomena of *self-organizing into subgroups* – this was apparent several times through 'recruitment' messages on the channel comments and group discussions, and it also represented itself in some media publications that it was indeed and activity that had emerged. This can be also articulated as saturation (Morse, 2017, p. 1392), where the increased number of evidence supports each other and increase the certainty of findings.

Reflexivity (Levitt et al., 2018), especially in ethnography where the researcher is the principal tool of research (Lincoln et al. 2017, p.246), is very important in gaining reliability and validity of research. In conjunction with the previous explanation of the effort of having multiple cases to represent a phenomenon, some reflective questions such as "How can I show this what I think is happening?"; "Did I need to make a large effort in retrospective analysis to show that a phenomenon exists? Why?"; "How does my previous knowledge and background influence what I am assuming?"; "What am I actually assuming here? Can I validate my assumptions?".

Validity and reliability would best have been improved by having multiple researchers conducting the study – thus the primary weakness was in fact that this research is the work of a single individual. This fact was known from the start of the research, and the method of mitigation was to at least gain external input from the network of the researcher comprising of both academics and practitioners in the field.

5 THE IT ARMY OF UKRAINE AS A COMPLEX ADAPTIVE SYSTEM

Describing a complex system inevitably begs a structure that is often a simplification of reality – an artificial construct – that represents the studied phenomena adequately. In this study too, decisions needed to be made on how to represent the findings in order to portray the Complex Adaptive System of IT Army of Ukraine in a logical manner. It was considered to structure this chapter at hand by using attributes of the ITAU as guiding structure and reflect them through the theoretical lens, i.e., size, operational methods, composition etc. However, during the analysis process it was noticed that the CAS Principles in ITAU were distinct enough to warrant the theory to guide the structure of the reporting of the findings.

While overlap exists both in the theoretical principles and concepts of CAS as well as in the attributes of the ITAU, this conceptual structuring was seen to provide the clearest possible way to articulate the properties of the system. Where applicable, these overlaps have been discussed in the following sections, while keeping the focus on the relevant principles that emerged from the findings. Table 4 represents the summary overview of the relevant CAS principles connected to the findings from the IT Army of Ukraine.

Table 4 Aggregated CAS principles with ITAU examples.

CAS principle	Description	ITAU
Adaptation/ Homeostasis	The ability of the system or its agents to adjust their behavior or structure in response to the changes in the environment or internal feedback (Holland, 1995; Levin, 1998; Chu et al. 2003; Buckley, 1968; Lewin, 1999; Anderson, 1999)	The ITAU adapts its tactics and targets according to the changing situation on the ground and the feedback from its members and allies.
Nonlinearity	The property that small changes in inputs or parameters can lead to large and unpredictable changes in the outcome or output of the system (Holland, 1995; Arthur et al.	A small-scale cyberattack by the ITAU can have a large impact on Russia's infrastructure or public opinion, such as disrupting power grids, spreading misinformation, or exposing corrup-

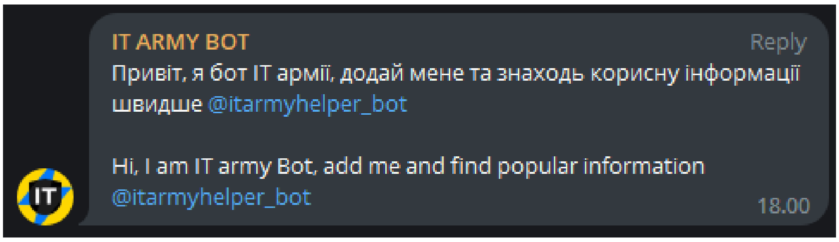
	1988; Cilliers, 1998; Buckley, 1968; Lewin, 1999)	tion.
Emergence	The phenomenon that new patters, structures, or behaviors arise from the interactions of the agent without being explicitly planned or programmed (Buckley, 1968; Lewin, 1999).	The ITAU in principle emerged from a grassroot movement of volunteers who wanted to defend Ukraine against Russia's aggression; it is low in formal structure, operated through self-organization and coordination. The collective cyber-attack capability and learning capabilities are emergent properties, which could not be achievable by a single individual.
Self-organization	The process by which order and coordination emerge from the local interactions of the agents without external control or direction (Holland, 1995; Cilliers, 1998; Buckley, 1968; Lewin, 1999)	The ITAU self-organized through a Telegram-channel where Russian targets were listed for volunteers to attack; self-organization also showcased through technical advising and learning and in formation of sub-groups.
Feedback	The mechanism by which information about the effects of actions or events is transmitted back to the source, influencing future actions or events (Holland, 1995; Levin, 1998; Buckley, 1968; Lewin, 1999)	The ITAU receives feedback from its members, allies, media, and adversaries about its cyberattacks; this feedback helps them evaluate their effectiveness, learn from their mistakes, and improve their tactics.
Diversity/ Individuality	The variety and uniqueness of the agents and their attributes, which enable them to perform different roles and functions (Holland, 1995; Levin, 1999; Buckley, 1968; Preiser et al. 2018)	The ITAU consists of thousands of diverse and individual volunteers with different roles, who have used a variety of methods and tools in participating in ITAU.
Cooperation/ Communication	The degree and quality of interaction and collaboration among agents, which can enhance collective performance and learning (Holland, 1995 (Tagging); Arthur et al. 1988 (Dispersed interaction); Cilliers, 1998 (Rich interaction of components).	The ITAU cooperates and communicates with each other through Telegram and website; they also cooperate with other Ukrainian institutions and loosely interact with other DDoS groups.
Co-evolution	The process by which two or more systems influence each other's evolution through mutual adaptation (Arthur et al. 1988; Buckley, 1968; Anderson, 1999).	The ITAU co-evolves with its targets in Russia, i.e. targets implementing DDoS protection; ITAU responding in utilizing VPN's from occupied territories to use geo-blocking against them, and using IP-Gate level targets instead of URL. ITAU and digital platforms seem to have a co-evolving element.
Openness/ Contextuality	The extent to which the system is influenced by and influences its environment, as well as its sensitivity to initial conditions and history (Cilliers, 1998; Chu et al. 2003; Preiser et al. 2018)	The ITAU is an open system to such extent that it's activities can be participated by monitoring its Telegram channel; it is influenced by and influences its environment; responds to the political military, and social situation in Ukraine and Russia; it also depends on its initial conditions and history.

5.1 Adaptation/Homeostasis

Adaptability is the ability of the system or its agents to adjust their behavior or structure in response to the changes in the environment or internal feedback (Holland, 1995; Levin, 1998; Chu et al. 2003; Buckley, 1968; Lewin, 1999; Anderson, 1999). The ITAU adapts itself based on the changing situation on the ground, and the feedback from its volunteers and based on its internal dynamics – representing also a kind of homeostasis.

The ITAU has adapted during its current lifespan of a little over a year. Some of these adaptations can seem simple and small, however they have played a large role in some of its principles of being a CAS. As an example, allowing participants to comment on the posts in ITAU Channel on 6th of March 2022 enabled more self-organization, adaptation and learning, cooperation, and feedback to emerge; while commenting ranged from less than ten comments to hundreds of comments depending on the post, the content reflected these aspects. Practical and repeated examples include asking and sharing technical advice, commenting and speculating how the targets are responding, and asking if there are actions or subgroups for more experienced volunteers.

Especially in the first months, the ITAU chat and channel comments were often filled with repeated comments and questions that were very similar to each other, and repeated topics such as "*is this appropriate tool for conducting DDoS*", "*How can I join*", "*What targets should I go first*", as well as technical and general questions about the group. In response to this, it was on 23th of March 2022 when the "IT ARMY BOT" appeared (Figure 3), which had the functionality in distributing basic information. While the basic questions indeed started seeminly lessen, it could also be attributed to the overall lessening of activity in the following months. Nevertheless, the implementation of the chatbot can be seen both as an adaptation to the pressure of information flow (questions) as well as being a homeostatic response, to assure the stability of the system, i.e., avoid becoming overwhelmed with questions and varying answers by participants in the chat group (Anderson, 1999; Levin, 2002; Lewin, 1999).



IT ARMY BOT

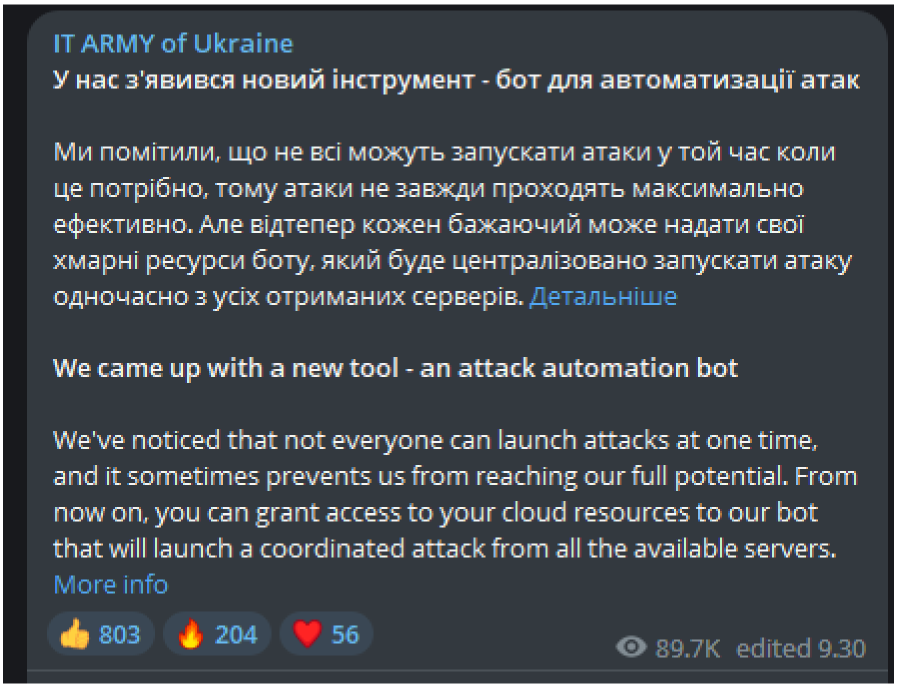
Привіт, я бот IT армії, додай мене та знаходь корисну інформації швидше @itarmyhelper_bot

Hi, I am IT army Bot, add me and find popular information @itarmyhelper_bot

18.00

Figure 10 ITAU Telegram Chatbot

On May 9th 2022 the IT Army of Ukraine started posting into the Channel and the Chat group that they have started offering a DDoS bot in order for volunteers to share their cloud-computing resources for ITAU DDoS attacks (Figure 11). On their first posts they articulated that this is due to the fact that they had noticed that the volunteers DDoS attacks could benefit from being synchronized. However, interestingly this also responds to the frequent questions and comments by the volunteers both in the channel comments and the chat, that spoke about having access or already using cloud services for the attacks. Much later it in fact became the "only" way for volunteers to operate.



IT ARMY of Ukraine

У нас з'явився новий інструмент - бот для автоматизації атак

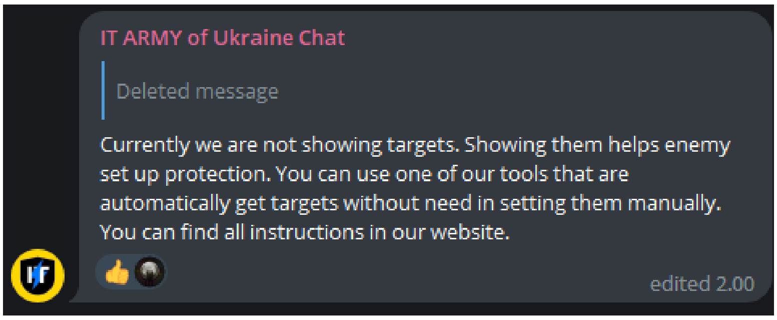
Ми помітили, що не всі можуть запускати атаки у той час коли це потрібно, тому атаки не завжди проходять максимально ефективно. Але відтепер кожен бажаючий може надати свої хмарні ресурси боту, який буде централізовано запускати атаку одночасно з усіх отриманих серверів. Детальніше

We came up with a new tool - an attack automation bot

We've noticed that not everyone can launch attacks at one time, and it sometimes prevents us from reaching our full potential. From now on, you can grant access to your cloud resources to our bot that will launch a coordinated attack from all the available servers. More info

Figure 11 Initiating bot for volunteer cloud services.

The ITAU worked for over a six months having especially the DDoS targets listed explicitly in the Telegram-channel, despite knowing that pro-Russian actors could well see them – as there were also incidents where seemingly pro-Russian actors tried to disseminate malicious content in the channel. However, the at 22.8.2022 the group implement an adaptation to the complex circumstances of apparent fact of both diminishing activity of the participants of the group, escalation and continous buildup of targets, as well as knowing that the possible targets could react based on the target lists, it was decided to discontinue the target listing (as seen in Figure 12). This shift of operating prodecure was implemented through centrally coordinating attack resources using ITAU developed DDoS tool and their website. This enabled the group to leverage automation of volunteer resources. Leveraging centrally-led automation in DDoS is a very known operating model that is more commonly attributed to the use of botnets (Deseriis, 2017).



IT ARMY of Ukraine Chat

Deleted message

Currently we are not showing targets. Showing them helps enemy set up protection. You can use one of our tools that are automatically get targets without need in setting them manually. You can find all instructions in our website.

edited 2.00

Figure 12 Articulating the discontinuing of target listing

In the spring of 2023, the adaptation of ITAU has been striving to position itself as an official part of the structure of Ukrainian military and create a way to have the volunteers of the organization to be considered a legal part of the ITAU (Waterman, 2023). While the underlying reasons for this are up for speculation more than explicit articulation, one can understand that the concerns that have been brought up in the larger spehere of discussion in public are one likely part of this move. One of the cornerstones of these concerns have been that the ITAU has been for the most part a "grey actor", where civilian individuals have taken part in different actions that are often considered illegal in their respective countries.

As a group the ITAU has changed considerably over the course of this study. While it still has several of the key characteristics that it had in the first few months of its conception, it has also lost some during the way. From the onset of the War in Ukraine, the ITAU stood out to be very open and organic, having more of a "direction of doing" than a very clear *how* and *what* it would be doing. While there were simple rules observed in the group, some more explicit and some more implicit than others – i.e., *conduct DDoS with any tools available against set targets*, *suggest targets preferably to the ITAU email*, *have technical advisory freely self-organize between volunteers*, and *moderate any pro-Russian actors out of the channel and group* – which created room for organic activity such as testing tools, having feedback, sharing information, sharing leaked data, etc. The overall mood of the group could have been articulated as having a sense of enthusiasm and "Do-It-Yourself" feeling, where learning tools and finding out that the volunteers could make an impact mattered.

Contrasting this to the latter months of 2022 and early 2023, the rules were more stricter – i.e., technical details should not be discussed, targets and especially their weaknesses should not be discussed, all targets are automated via the ITAU webpage/bot-system, channel is used mostly for post-operation reporting of results, and demarcation of those that get to be volunteers through the application form[4] and those that are basically just contributing their computational resources to ITAU.

[4] IT ARMY Volunteer Questionnaire: https://docs.google.com/forms/d/e/1FAIpQLSfdSnn52XhhkFPc3dQ-QKpifYyJU0Td8n0h9oYPeFHg2CM-vw/viewform

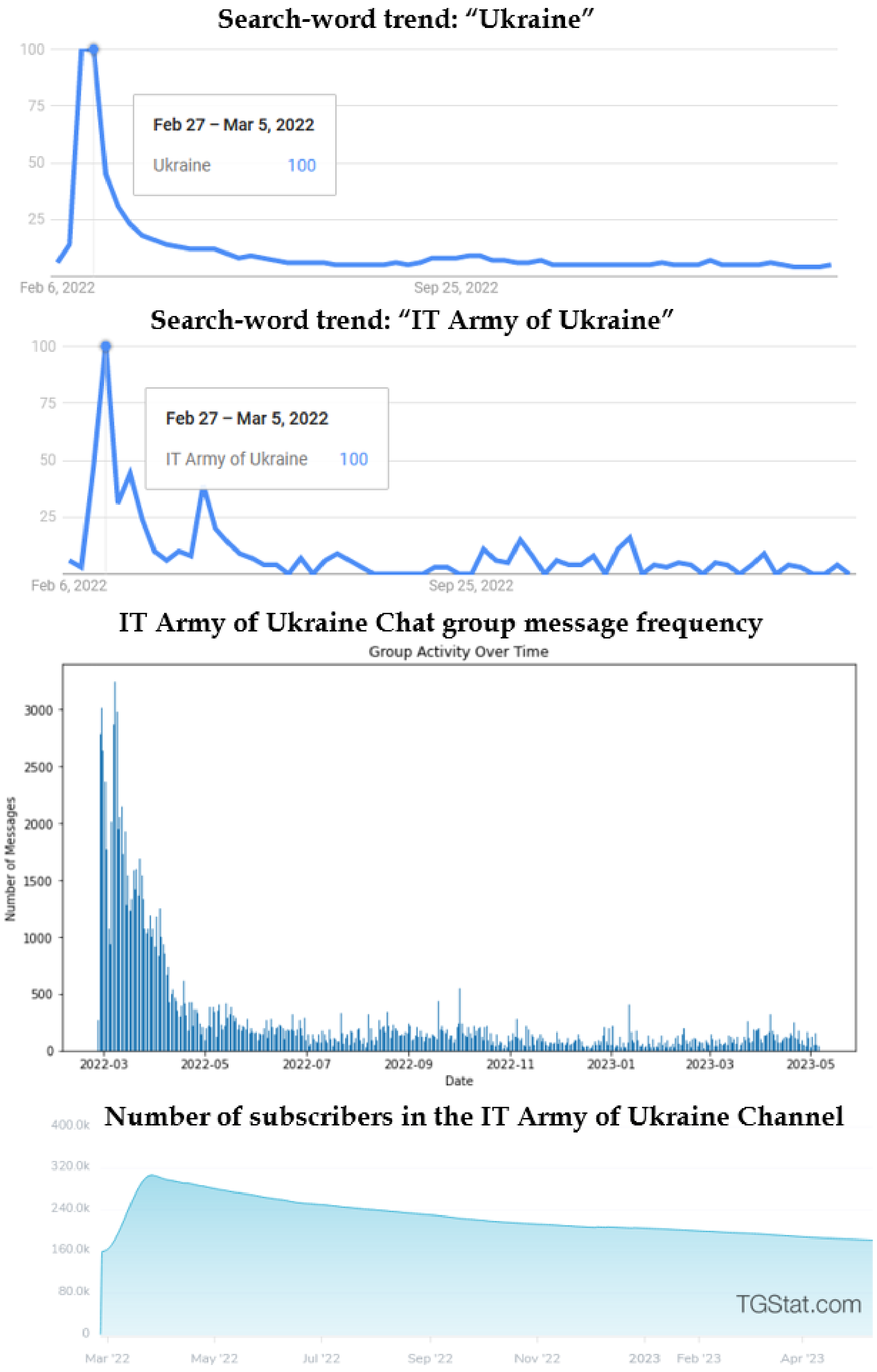
In the context of CAS, the term co-evolution emphasizes the co-dependence that two (or more) systems showcase when they are evolving through time. However, could these changes in ITAU be "mirrored" in some way in some other system? If the Russian ecosystem of targets is thought as one system, then the case could be argued that many of the changes in ITAU are due to answering challenges such as not giving the targets time to prepare, and not enabling them to improve their defenses by monitoring the feedback and discussions in ITAU. Also, it could be said that changes are also due to hardening ITAU against possible retaliation from the pro-Russian actors. While these are sometimes explained as reasons by a few active members of ITAU in their chat group and channel, there is also one very pragmatic and realistic reason that could be underlying for many of the changes, and have to do more with the environment – which also can be thought of as a system, i.e., the global society (Easton, 1968, p. 431) – and the dynamics of the entire war itself.

In Figure 13 there are charts[56] for comparison that are relevant for understanding the dynamics of ITAU. In the first two graphs, the frequency of Google searches on topics "IT Army of Ukraine" and "Ukraine" can be compared with next two the message-frequency of the ITAU chat-group[7] and the number of the channels subscribers. The patterns are strikingly similar; the more interest the public has with the War in Ukraine and the IT Army of Ukraine, the more activity in the ITAU Telegram. The downward shifts after the initial period of torrent of activity are not due to things such as ending the target-listing, since that occurs later in August 2022. It could in fact, be more of the opposite. Having their numbers and activity levels dwindle, at least in discussion-wise (actual DDoS capability is unknown), from a purely technical perspective the shift to automation and centralization can bring efficiencies that counterbalance the lesser numbers of volunteers. There can still be tasks that require more skills and abilities from a human operator, and thus the capitalization of the possible talent pool by utilizing the recruitment form is very logical.

[5] For Google trends: https://trends.google.com/trends/explore?date=2022-02-01%202023-04-30&q=IT%20Army%20of%20Ukraine&hl=en-US

[6] For ITAU Telegram channel stats: https://tgstat.com/channel/@itarmyofukraine2022/stat/subscribers

[7] Message activity was analyzed using the researcher's own solution based on Python (Panda & PyPlot)



Search-word trend: “Ukraine”

Search-word trend: “IT Army of Ukraine”

IT Army of Ukraine Chat group message frequency

Number of subscribers in the IT Army of Ukraine Channel

Figure 13 The comparison of Google trends and ITAU activity

The group has had a linear downturn in subscribers to the ITAU Channel according to TGStat (TGStat, n.d.), which for the most of the life of ITAU served for listing targets, results, and other information. The numbing of the novelty-sense of the War in Ukraine as in many other conflicts before that, can be at the very least be speculated to have lessened the intrest towards the IT Army of Ukraine. And with less numbers of new participants in the chat-group, the less there are posted messages. While the lessening of activity in the chat-group can also be due to shifts in tactics and operations, as well as already having a formidable amount of basic information in the past discussions, the similarity in trendlines is still plain to see.

As mentioned earlier, especially during the initial 3 months when the group was having its initial spree of activity that can be also seen clearly in the chart found in Figure 13 mentioned earlier, many technically oriented people self-organized themselves into subgroups that focused more on things such as SQL-injections and breaking into information systems. Seeing perhaps potentially skilled volunteers drifting to subgroups, the previously mentioned volunteer-form for drawing them deeper into the ITAU by a recruiting process is also logical, however unfortunately speculative, conclusion. Gaining deeper knowledge into the drivers of decisions that influenced the evolution of ITAU would be an excellent opportunity for further research. This also changed the cyber kill-chain (Lockheed Martin, 2023) of the ITAU (Table 5). The ITAU cyber-kill chain presented is based on the Lockheed Martins (2023) chain and is structured from the information that is perceivable during the research from the group, and represents more of a summary than all the details and nuances. As an example, the ITAU most likely has internal / partnered intelligence capability, which is not represented in the table.

Table 5 ITAU Cyber Kill Chain changes

Original Cyber Kill Chain of ITAU	**Later Cyber Kill Chain of ITAU**
1. Encourage anyone to start DDoS against Russia to defend Ukraine	1. Encourage anyone to offer their resources to DDoS Russia to defend Ukraine and recruit IT capable individuals
2. Gain public suggestions for new targets from the volunteers, closed suggestions through email	2. Closed suggestions through email.
3. Publish target lists of Russian websites and services	3. Give technical advice on how to connect volunteer resources for automated DDoS
4. Enable discussion on technical and operational aspects	4. Post results of attacks with moderation
5. Attacks are commenced by volunteers independently	5. Enable discussion but limit technical and operational details
6. Results are posted and discussed openly	

5.2 Nonlinearity

The property that small changes in inputs or parameters can lead to large and unpredictable changes in the outcome or output of the system (Holland, 1995; Arthur et al. 1988; Cilliers, 1998; Buckley, 1968; Lewin, 1999). A small-scale cyberattack by the ITAU can have a large impact on Russia's infrastructure or public opinion, such as disrupting power grids, spreading misinformation, or exposing corruption – while also few individuals giving technical advice can cascade into a culture of helpful commenting.

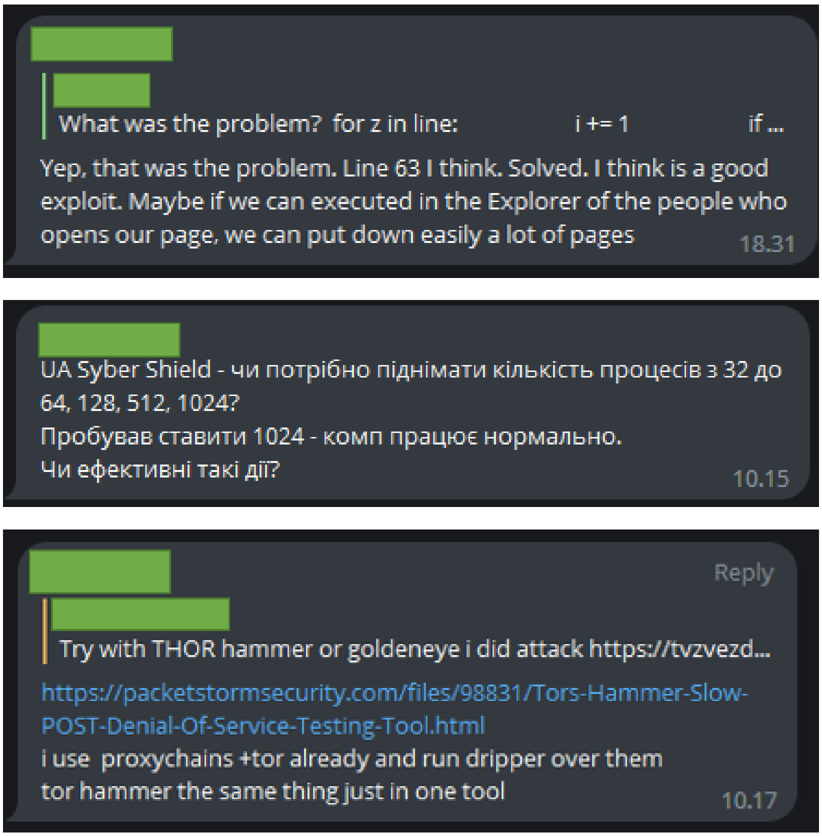
When the ITAU started to focus their DDoS attacks on the banking sector, starting from general websites and moving into ATMs, then mobile banking, and finally even to crypto-currecy traders, some pieces of information showcased how their actions could have unplanned and unpredictable outcomes. This was the delayed payments of the RU military and drafter personnell (Ankel, 2022; Cole, 2023).While this event could have components other than relating to the actions of the ITAU, the reports of Russian military bloggers and open videos of russian drafted personnell coinciding with said attacks make an interesting coincidence. The drafted personnell were indeed lamenting that they have been lied to, and no promised payments have been made. Having already malfunctioning drafting system and difficulties of having enough proper manpower, this type of public messaging especially since it could be interpreted as treason, is a setback for the Russian side.

Not long after this, the ITAU started explicitly targetting some financial institutions that were known to solicitate payments to draftees and volunteers on the Russian side of the war. It is thus possible, that either the Ukrainian side had information that this indeed was the impact that their operation had, or they interpreted it based on those public outcries. Nevertheless, this showcased at least the potential of nonlinear outcomes that a relatively limited DDoS attack might cause – especially since ITAU target-lists have been previously posted in other DDoS groups, expanding their capabilites often in unpredictable ways.

5.3 Emergence

Emergence in complex adaptive systems refers to the phenomenon where small changes in inputs or parameters can lead to large and unpredictable changes in the system's outcomes or outputs (Holland, 1995; Arthur et al. 1988; Cilliers, 1998; Buckley, 1968; Lewin, 1999). The IT Army of Ukraine (ITAU) itself can be seen as an emergent entity, originating from a grassroots movement of volunteers intent on defending Ukraine against Russian aggression. Despite its lack of obviously formal structure or leadership, the ITAU operates effectively through self-organization and coordination. Its collective cyber-attack capability is an emergent property, far exceeding what could be achieved by any single individual.

A key example of emergence in ITAU can be seen in its cyber-offensive capability. Drawing an analogy with an ant colony, a single ant may process less information than a solitary ant. However, as part of the collective, each ant contributes to a vastly superior computation capability (Lewin, 1999, p. 175). Similarly, the actions of a single ITAU volunteer launching a DoS/DDoS attack might have minimal impact on a website. Yet, when hundreds of such volunteers act in concert, using diverse approaches, they can create a significant impact. Likewise, one person offering technical advice might not significantly influence the group's overall capability, but when this behavior becomes a part of the group culture, it can spur the emergence of self-learning, self-correction, and adaptability. This culture of sharing advice was evident in both the ITAU Channel comments and the Chat group (Figure 14). It also manifested in the willingness of members to independently develop tools and techniques for conducting cyber-attacks on targets.



[redacted]

> [redacted]
> What was the problem? for z in line: i += 1 if ...

Yep, that was the problem. Line 63 I think. Solved. I think is a good exploit. Maybe if we can executed in the Explorer of the people who opens our page, we can put down easily a lot of pages 18.31

[redacted]

UA Syber Shield - чи потрібно піднімати кількість процесів з 32 до 64, 128, 512, 1024?
Пробував ставити 1024 - комп працює нормально.
Чи ефективні такі дії? 10.15

[redacted]

> [redacted]
> Try with THOR hammer or goldeneye i did attack https://tvzvezd...

https://packetstormsecurity.com/files/98831/Tors-Hammer-Slow-POST-Denial-Of-Service-Testing-Tool.html
i use proxychains +tor already and run dripper over them
tor hammer the same thing just in one tool 10.17

Figure 14 ITAU Technical discussions of volunteers[8]

Collective learning suggests that the property of emergence in ITAU is not merely a theoretical concept, but a tangible attribute that significantly shapes the group's operational capability.

[8] Translation: *UA Syber Shield - is it necessary to increase the number of processes from 32 to 64, 128, 512, 1024? I tried to set 1024 - the computer works fine. Are such actions effective?*

5.4 Self-organization

The process by which order and coordination emerge from the local interactions of the agents without external control or direction (Holland, 1995; Cilliers, 1998; Buckley, 1968; Lewin, 1999). The ITAU self-organized through a Telegram-channel where new Russian targets are listed for volunteers to attack; it also collaborates with officials from Ukraine's defense ministry and other cyber groups.

The self-organization aspect has been a hallmark of the ITAU from its first days. One notable aspect of the self-organization has been the appearance of sub-groups that have emerged as more covert offshoots of the ITAU. Several examples were seen where individuals who wanted to leverage their skills in a different attack vector tried to form their own groups to carry of attacks with for example, SQL-injections; "*Are there anyone who wants to create a subgroup for targetting exploits?*". Some participants articulated already having formulated a sub-group, and wished to coordinate their activities with the more formal, behind-the-scenes ITAU activities "*We have a subgroup and are interested in cooperation – could the moderator Private Message*?".

The target-listing of ITAU served to enable a self-organizational aspect of DDoS attacks, and in non-linear way that could have even been unforseen by the founders of ITAU. This is especially the case where the targets got listed in groups that were loosely coupled to the ITAU, but that at least through the target-listing became part of the larger ecosystem of DDoS attacks. Some other notable Telegram chat groups include DDoS Joint Group, Hacker Forces, Studentcyberarmy, CyberFire, disBalancer Ukraine, disBalancer English, KiberBull, DDoS Attack Cyber Cossacks, and Cyber Cerber.

The self-organizing aspect of ITAU came also through its self-moderation: participants frequently reported and verbally attacked posts and those posting them if they perceived that they were either disseminating pro-Russian content or directly violating either explicit or implicit rules of the group, such as trying to recruit into cyber-capable people to IT companies.

5.5 Feedback

Feedback, or feedback-loops are the mechanism by which information about the effects of actions or events in or about the system is transmitted back to the source, influencing future actions or events (Holland, 1995; Levin, 1998; Buckley, 1968; Lewin, 1999). The ITAU received feedback from its members, allies, media, and adversaries about its cyberattacks; this feedback helps them evaluate their effectiveness, learn from their mistakes, and improve their strategies. Feedback-mechanism in ITAU were essential in order for it to adapt and evolve. Feedback should not be understood solely as feedback that a person gives explicitly – feedback could manifest itself through continuously hardening targets in its environment, or volunteers seeing how others are giving out technical advice – compelling them to join giving similar advice as well.

Prior to the de-listing of its targets, the ITAU had a visibly more complex feedback-loop mechanism than after it implemented the de-listing (automation) of targets. In general, the ability to utilize feedback loops has a strong impact on the system's ability to adapt to stress (Easton, 1968, p. 434); while the public discussion of targets was removed and it might hinder a positive feedback loop, it is possible that a similarly strong feedback loop has been developed inside ITAU, which is invisible to the outside observer.

In Table 6, the changes in the feedback-mechanism from the perspective of the volunteers participating in the public discussion. While the feedback loop of might in very similar fashion still remain in the "invisible" part of the ITAU, from the public perspective it has changed so that the majority of the agents in the system – volunteers in Telegram – cannot be a significant part of the feedback loop. If the volunteers are not able to discuss the targets, some other elements such as ethical reflection might be sidelined in the overall operation. Also, the experiences of participation can change into more monotonous role if they perceive themselves to be merely a tiny part of the cog in the large DDoS mechanism.

Table 6 Changes in the feedback-mechanism involving public discussion.

Pre-delisting of targets	**Feedback**	**Post-delisting of targets**	**Feedback**
Target-lists with pre-operation information	Volunteers commenting pre-ops and post ops	No lists	No pre-ops feedback or information
Post-operation posts	Volunteers commenting post-ops, detailed, technical	Post-operation posts	Post-ops comments limited, general
Perceived target impact during operations	Volunteer comments in channel during and post-ops	Targets unknown	No comments
Target responding / evolving	During and post-ops comments, advice from volunteers in channel and discussion	Unknown targets	No comments
Public discussions about targets	Posts, comments, on targets post-ops.	Public discussions about targets	Posts, comments, on targets post-ops.

5.6 Diversity/Individuality

The variety and uniqueness of the agents and their attributes, which enable them to perform different roles and functions (Holland, 1995; Levin, 1999; Buckley, 1968; Preset et al. 2018). The ITAU consists of thousands of diverse and individual volunteers and participants. When looking at the different agents of ITAU, the primary agents are clearly the individual persons that are part of the organization – whether tightly or more loosely coupled (Perry, 2010). The individuals inside the official structure of ITAU, the ones that are more direct part of the governmental structure and who organize and administer the group are practically invisible for inspection. What however can be articulated, is that these individuals most likely have a varying degrees of roles that differentiate them, but also with some certainty that their roles being inside the ITAU makes the quite different to the more loosely coupled individual volunteers that act through the Telegram channel and the website.

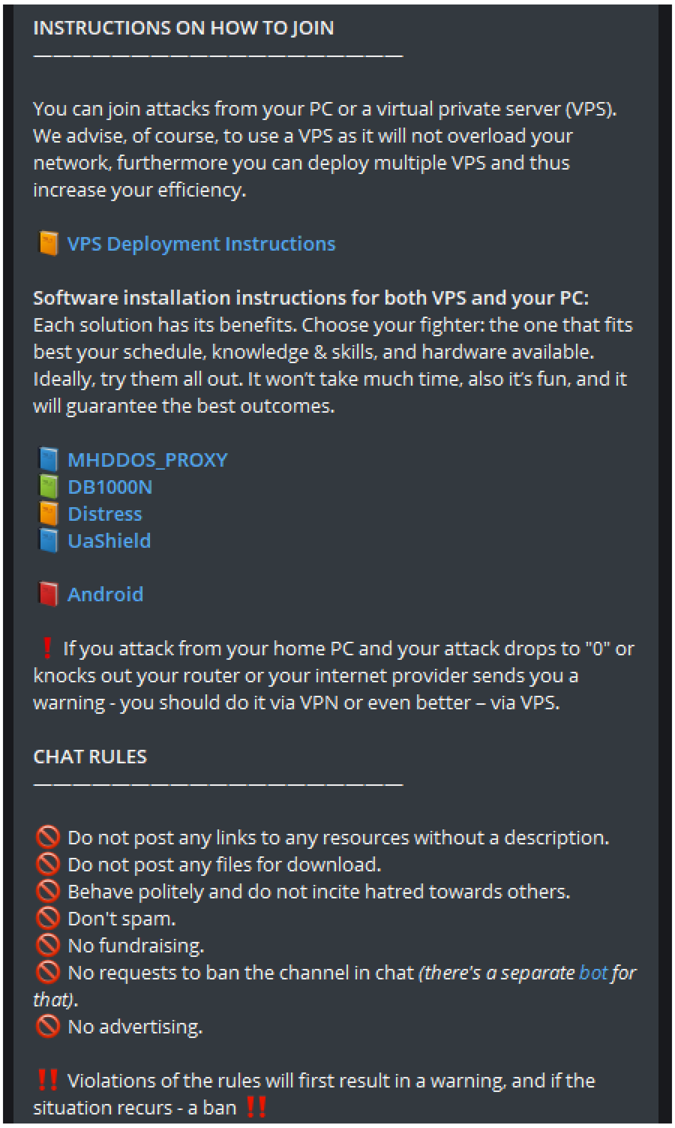
As an example, the access to information and understanding the groups activity and resources must be on a level that enforces more discretion than a person who has only access to resouces and information that are already publicly available. Here, the diversity aspect of a CAS can be seen to be very much akin to almost any organization that has individuals with varying roles and functions.

Individuality of people can be taken granted to atleast some extent, which can play a significant role in ITAU as a CAS. One way of seeing the diversity of people in the volunteer corps of the ITAU is the diverse input of offers to help, where the messages often incorporate either seemingly useful job-background or the complete opposite but high willingness to do something.

The freedom of action that the group provides has also sprung activities outside of DDoS, where the diverse individuals have been enabled to use their different skills and attributes to use – as an example dispersing leaked information, contact details, and reporting vulnerabilities. The diverse set of volunteers can also be perceived from the different opinions that are raised about the listed targets and used methods. The most notable ethically challenging event was the listing of Russian pension funds, which is opened more on the section 5.9 Openness..

An example of the ethical dilemmas the volunteer faced is well apparent from some volunteers who openly asked "*Are there ways to help which are legal?*", since they felt, often rightly, that using DDoS or other hacking tools were illegal at least in their respective countries. This type of illegal-legal discussion was however scarce. Yet, considering that this is a genuine issue, it can be said that this fact remained a constraint on some individuals when considering whether to join the actions or not. The extent to which this might have influenced the size of the group, is however unclear.

Especially in the initial stages of ITAU, diverisity became apparent from the different tools that the volunteer were using for DDoS attacks and also from the multiple variations and modifications that went along with them. Some of the tools that were mentioned included *Slowiris*, *Manyloris*, *Low Orbit Ion Cannon* (aka LOIC), and *High Orbit Ion Cannon* (aka HOIC), and DDoS Ripper. However, the main tools of the trade became *db1000n* (Death by 1000 Needles), *MHDDoS*, and *uashield* (UA Cyber Shield), which started to be actively promoted by the ITAU (Figure 15). The varying levels of individual skills and motives combined with the different tools already point clearly out the wide range of diversity the ITAU had.



INSTRUCTIONS ON HOW TO JOIN
————————————————————

You can join attacks from your PC or a virtual private server (VPS). We advise, of course, to use a VPS as it will not overload your network, furthermore you can deploy multiple VPS and thus increase your efficiency.

📙 VPS Deployment Instructions

Software installation instructions for both VPS and your PC:
Each solution has its benefits. Choose your fighter: the one that fits best your schedule, knowledge & skills, and hardware available. Ideally, try them all out. It won't take much time, also it's fun, and it will guarantee the best outcomes.

📘 MHDDOS_PROXY
📗 DB1000N
📙 Distress
📘 UaShield

📕 Android

❗ If you attack from your home PC and your attack drops to "0" or knocks out your router or your internet provider sends you a warning - you should do it via VPN or even better – via VPS.

CHAT RULES
————————————————————

🚫 Do not post any links to any resources without a description.
🚫 Do not post any files for download.
🚫 Behave politely and do not incite hatred towards others.
🚫 Don't spam.
🚫 No fundraising.
🚫 No requests to ban the channel in chat *(there's a separate bot for that).*
🚫 No advertising.

‼️ Violations of the rules will first result in a warning, and if the situation recurs - a ban ‼️

Figure 15 IT Army of Ukraine post on general instructions

5.7 Cooperation/Communication

The degree and quality of interaction and collaboration among agents, which can enhance their collective performance and learning (Holland, 1995; Arthur et al. 1988; Cilliers, 1998. The ITAU cooperates and communicates with each other through Telegram and website; they also most likely cooperate with other branches of the Ukrainian military and government, and have loosely-coupled (Perry, 2010) connections with other hacker and DDoS groups.

The ability for the volunteers in the ITAU channel and group to communicate with each other enabled a "zone of proximal development" (Vygotsky, 1978) for those members of the group that for example lacked basic technical skills to participate in DDoS attack or who lacked even the basic understanding of what the DDoS is based on. The commenting in the channel and the discussions in the chat-group allowed dissemination of best practices, technical scripts, technical help, target spesific tips etc. Some users quickly self-organized into roles, who frequently gave technical advice.

Quick communication allowed also the formation of sub-groups, but also had the side-effect of so-called "recruiters" who were hunting for services or talented tech-savvy people to join either in their projects or to companies. Some even tried to market their own services and projects to be disseminated via the group or even through attacks. This led to the swift moderation of this type of behavior.

Open communciation also made it possible for pro-Russian actors to either visibly post harassing messages to the group, or to give malicious technical scripts and programs. There was even a malicious DDoS-tool launched, which was targeted for the ITAU members to use and was shared by some accounts as a Zip-file accompanied by seemingly credible use-instructions; in actuality it also gathered information of its user (Toulas, 2022). The tool mimicked the tool called DisBalancer which was designed by Hacken Foudation in 2021 for decentralized DDoS protection – however, the tool was re-designed to use the same method for conducting DDoS and re-labeled as "Liberator" (Disbalancer, 2022). The open format of the ITAU proved also to be a weakness, and later in its development the openness was limited by moderating certain topics of discussion – such as target info and detailed technical information. Also, on an operational sense, the ITAU adapted into using closed and automated target lists, instead of open target lists.

Communication with other DDoS groups was also evident, since the same target lists were shared and forwarded into other groups such as Hacker Forces[9], Student Cyber Army[10], Cyber Palyanitsa[11], DDoS Attack Cyber

[9] Hacker Forces: https:// t.me/hackencyberarmy/

[10] Student Hacker Army: https://t.me/studencyberarmy/

[11] Cyber Palyanitsa: https:// t.me/CyberPalyanitsa/

Cossacks[12] and the Ukrainian Reaper[13]. While the relationship between the groups is uncertain, it has been evident that other groups are known to promote same targets as the IT Army of Ukraine, which could quickly have non-linear consequences due to the fact that at the time of writing on 25th of March, the groups in total numbered over 10,000 subscribers, and these are not the only known groups conducting hacking and DDoS attacks against Russian targets.

5.8 Co-evolution

The process by which two or more systems influence each other's evolution through mutual adaptation (Arthur et al. 1988; Buckley, 1968; Anderson, 1999). The ITAU co-evolves with its targets in Russia, i.e. targets implementing geo-blocking and reverse-proxy protection; ITAU responding in utilizing VPN's from occupied territories to use geo-blocking against them, and using IP-Gate level targets instead of URL. Russian cyber groups have mimicked ITAU operations (e.g. IT Army of Russia).

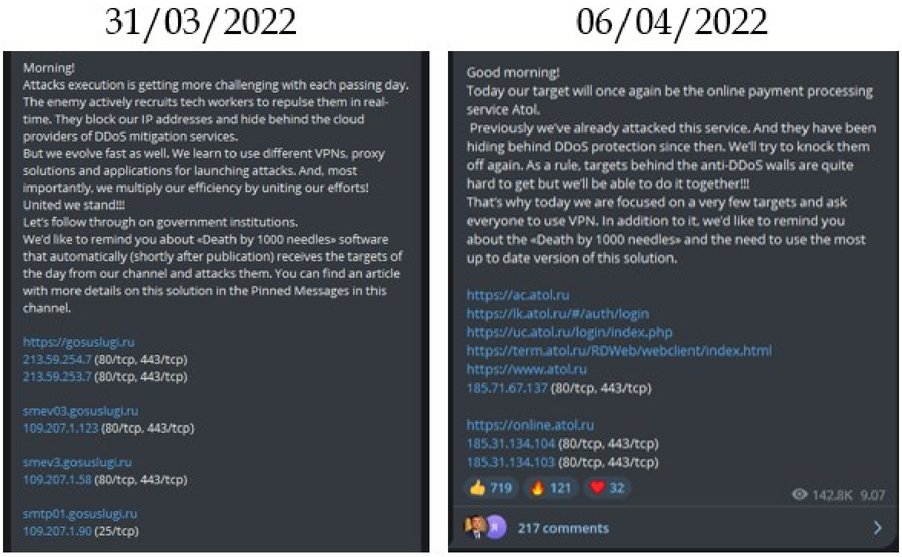
The ITAU has co-evolved most in respect to its targets, where at first the simple method of listing urls and IP addresses was sufficient to make an impact ot the targets. However, many websites started to adopt reverse-proxy protection, and some used different types of geo-blocking of IP ranges. While reverse-proxy was sometimes bypassed by usign only IP-addresses and spesific gates to point the attack, geo-blocking was bypassed by encouraging to always use VPN services that were inside Russia.

One interesting result of the geoblocking of IP-ranges was the services located in occupied zones, or users that were in occupied zones. This in fact made it possible to either seem like malicious traffic was coming from the occupied zone to Russia, or from Russia to the target in the occupied zone. Applying geo-blocking by the targets quickly resulted in either having the occupied resource being unable to have any users access it from Russia, or blocking users from the occupied zones from accessing resources in Russia.

This "arms race" has the side-effect of hardening Russian services from future DDoS attacks. Examples can be seen from 31st of March 2022 and April 6th 2022 (Figure 16), where the ITAU Channel is already posting that previous targets have started using DDoS-protection. Hardening targets can naturally prove to be a counter for the operations of ITAU – which were bypassed by using different methods. However, using more resources for hardening in Russia is bringing additional costs to a society which is already under significant pressure due to the war.

[12] DDoS Attack Cyber Cossacks: https:// t.me/ddos_separ/

[13] Ukrainian Reaper: https:// t.me/ukrainian_reaper_ddos/



31/03/2022

Morning!
Attacks execution is getting more challenging with each passing day. The enemy actively recruits tech workers to repulse them in real-time. They block our IP addresses and hide behind the cloud providers of DDoS mitigation services.
But we evolve fast as well. We learn to use different VPNs, proxy solutions and applications for launching attacks. And, most importantly, we multiply our efficiency by uniting our efforts!
United we stand!!!
Let's follow through on government institutions.
We'd like to remind you about «Death by 1000 needles» software that automatically (shortly after publication) receives the targets of the day from our channel and attacks them. You can find an article with more details on this solution in the Pinned Messages in this channel.

https://gosuslugi.ru
213.59.254.7 (80/tcp, 443/tcp)
213.59.253.7 (80/tcp, 443/tcp)

smev03.gosuslugi.ru
109.207.1.123 (80/tcp, 443/tcp)

smev3.gosuslugi.ru
109.207.1.58 (80/tcp, 443/tcp)

smtp01.gosuslugi.ru
109.207.1.90 (25/tcp)

06/04/2022

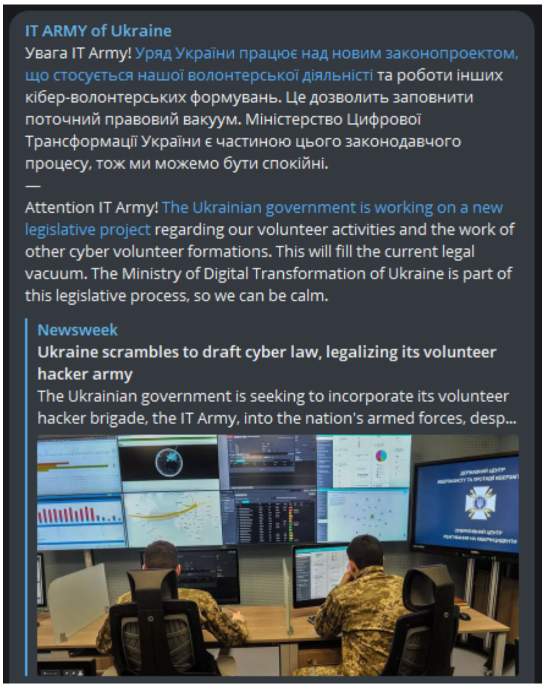
Good morning!
Today our target will once again be the online payment processing service Atol.
Previously we've already attacked this service. And they have been hiding behind DDoS protection since then. We'll try to knock them off again. As a rule, targets behind the anti-DDoS walls are quite hard to get but we'll be able to do it together!!!
That's why today we are focused on a very few targets and ask everyone to use VPN. In addition to it, we'd like to remind you about the «Death by 1000 needles» and the need to use the most up to date version of this solution.

https://ac.atol.ru
https://lk.atol.ru/#/auth/login
https://uc.atol.ru/login/index.php
https://term.atol.ru/RDWeb/webclient/index.html
https://www.atol.ru
185.71.67.137 (80/tcp, 443/tcp)

https://online.atol.ru
185.31.134.104 (80/tcp, 443/tcp)
185.31.134.103 (80/tcp, 443/tcp)

Figure 16 Targets hardening in Russia

At the time of writing this thesis, the Ukrainian government announced that they have started a legislative project in order to fit the volunteer activities of the ITAU into the official military structure of Ukraine (Waterman, 2023), something that it lacked possibly due to its ad-hoc creation. Same news was also posted in the ITAU Channel as seen in Figure 17. While this process would most likely be a necessary step in the creation of a cyber-force, the move could also be seen to be in response to the group being in the grey-zone: not a military but not a civilian organization, not specifically Ukrainian but not entirely internal either.



IT ARMY of Ukraine
Увага IT Army! Уряд України працює над новим законопроектом, що стосується нашої волонтерської діяльності та роботи інших кібер-волонтерських формувань. Це дозволить заповнити поточний правовий вакуум. Міністерство Цифрової Трансформації України є частиною цього законодавчого процесу, тож ми можемо бути спокійні.
—
Attention IT Army! The Ukrainian government is working on a new legislative project regarding our volunteer activities and the work of other cyber volunteer formations. This will fill the current legal vacuum. The Ministry of Digital Transformation of Ukraine is part of this legislative process, so we can be calm.

Newsweek
Ukraine scrambles to draft cyber law, legalizing its volunteer hacker army
The Ukrainian government is seeking to incorporate its volunteer hacker brigade, the IT Army, into the nation's armed forces, desp...

Figure 17 Post in ITAU Channel about officializing ITAU

While legitimizing the group into the structure of the Ukrainian military, it might not solve all the legal concerns that comes from participating in its activities, which is an issue that has been raised repeatedly in the public (Milno, 2022). In terms of co-evolution, if the ITAU becomes an official part of the Ukrainian military, it might force other institutions and the public to reconsider how they perceive the actions of the organization.

The IT Army of Ukraine started operating its website *itarmy.com.ua* on 5.4.2022. Very early on the site was protected by CloudFlare, a company that offers specialized services such anti-DDoS protection. This is an interesting nuance, since ITAU is largely based on conducting DDoS attacks. In addition to this, ITAU has from the start relied on Google Gmail[14] as its email provider. Both of these facts can be considered interesting, since in many cases the actions of ITAU could have been seen if not directly illegal, at least breaching terms of service.

Following in similar manner, the fact that many of the repeatedly referenced DDoS tools in ITAU Channel and Chat are hosted in GitHub repositories, begs the question how GitHub and in extent Microsoft (as the owner of GitHub), allow these tools to exist in their repositories? Some tools could be said to have the explicitly stated purpose of education or stress/penetration testing - MHDDoS articulates that it should not be used against website without the owner's consent[15] and UA Cyber Shield states that they do not support unlawful attacks[16]. However, both are used extensively by the ITAU (and similar actors) for the purpose of running DDoS campaigns. Are large digital corporations willingly turning a blind eye on the operations of ITAU?

If this is the case, there can be said to be co-evolution taking place where the emergence of ITAU in its context has in turn changed the digital platform corporations to willingly bypass their own terms of service. In general, since platforms such as Google generally forbid their services to be used in illegal purposes such as DDoS, some members are facing this from an individual perspective as they reported numerous times that they have been notified of conducting DDoS by Google in breach of terms of service. However, following similar logic, the ITAU using not only Gmail, but also Google Drive, should at this point be denied[17].

[14] IT Army of Ukraine Gmail: armyuait@gmail.com

[15] MHDDoS: https://github.com/MatrixTM/MHDDoS/blob/main/README.md

[16] Uashield: https://github.com/opengs/uashield/blob/master/README-en.md

[17] The author of this thesis has worked in a subcontractor that has in fact searched, analyzed, and tagged for moderation those resources that have had content and activity that has breached Google terms of service. Hosting instructions and using the platform for DDoS would be a violation of said terms of service.

5.9 Openness / Contextuality

Openness as a property is the extent to which the system is influenced by and influences its environment, as well as its sensitivity to context: initial conditions and history – it's a product of its context (Cilliers, 1998; Chu et al. 2003; Preiser et al. 2018). The ITAU is an open system to such extent that it's activities can be participated by joining and monitoring its Telegram channel; it is also influenced by and influences its environments; it responds to the political military, and social situation in Ukraine and Russia; its trajectory is also dependent on its initial conditions and history.

In complexity science, the concept of *initial conditions* stems largely from the core of chaos theory (Lorentz, 1972), which is sometimes articulated as one branch of complexity science (Raisio & Lundström, 2017). While in mathematical terms, when initial conditions are known precisely enough, the behavior of the system can be predicted – the more precisely known, the more accurately the predictions become (Lorentz, 1972). However, the broader complexity science, as well as the notion of complex adaptive systems, take it implicitly and granted that we can never have enough knowledge of all the variables and states in a system that its behavior could be precisely predicted (Luoma & Lindell, 2020; Marion & Uhl-Bien, 2001; Uhl-Bien & Marion, 2009). This is especially true in organizational context – how could it be possible to know every detail of every person at the birth of ITAU, for example? This makes our knowledge inherently limited, or as Herbert Simon (1997) expresses, we have to operate with *bounded rationality*.

The context where ITAU operates is linked directly to the initial conditions of its founding. To understand a complex adaptive system, the contextuality it operates in is of vital importance. With CAS, using generalization is often an ineffective tool – knowledge of the system is largely context dependent (Richardson & Cilliers, 2001). The initial conditions and the context were, and to an extent still are, that ITAU is a Telegram-coordinated, volunteer-based organization, created in immediate response to the illegal attack of the Russian Federation against sovereign state Ukraine and which uses any attack vector possible in the cyber-domain against the state and society of Russia. This initial condition and context defined the path of the organization from the very start, and which could be perceived to resonate during the study of the organization.

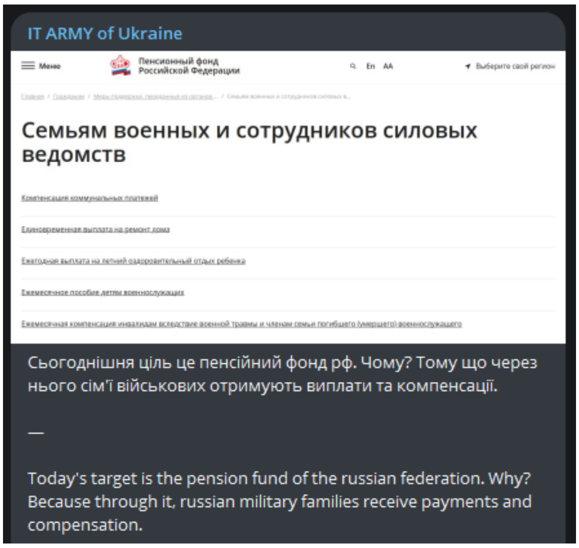
However, while the stage is now set in general terms, the initial conditions and context need to be decomposed to their parts in order to lay out what they were observed in practice. This is represented in Table 7.

Table 7 Initial conditions and context of ITAU

Initial conditions and context	**In practice**	**Result**
Telegram-coordinated	Telegram-coordination made it technologically possible to have a scalable way to transfer information (targets, technical information, coordination). Being open and easily accessible despite of tools, skills, and abilities: internet connection and an endpoint device such as a smartphone were succinct, it made quick participation in extensive scale possible.	Size and structure
Volunteer-based	Being volunteer-based from the start, any person irrespective of location, background, or ability could join the action immediately.	Size and structure
Immediate response	The fact that the group was created in a manner of days within the attack of Russian Federation, took leverage of the extremely wide coverage of the start of the war and strong backlash against it. This can be perceived from the trendline of both Google results, and message activity and number of subscribers to the group; Google trend and message activity go together.	Size, methodology
Illegal attack of Russian Federation against the sovereign state of Ukraine	The illegality of the Russian attack, which resulted from the first day in civilian casualties, gave the group ethical stance of being on the "right side" of the war.	Size, continuous basis for operations.
Any attack vector in the cyber-domain	Any attack vector, which is what the Ukrainian Minister of Digital Transformation stated in the launching tweets and Telegram messages gave a self-organizing and freedom of movement for those that were willing to participate. Thus, the level of technological know-how and ways to conduct attacks were not set by the group but the participants themselves. "Do what you can."	Size, operational logic, tactics, variety in attacks.
Against state and society of Russia.	Since from the start and continuing to current date, the target of operations were the State of Russian Federation as well as the society as a whole, it gave nearly infinite number of targets available and created a perspective where there were very little in constraint on what tools to use, how to use them, and to what to use them against.	Operation logic, effects.

Contextuality in the context of CAS means that the development of the system is heavily influenced by its specific context (Cilliers, 1998), i.e., if having the underlying war been somewhere else and including different regional dynamics, the context of the development of ITAU would have most likely been very different. One aspect of the contextuality can be perceived through the lens of seeing the Russian invasion as illegal and ethically very condemnable – which on the flip side makes the actions of ITAU by its member seen very justified. However, to highlight this one need to search for the boundaries of ethical consideration, because ethics clearly play a role in what and how ITAU functions.

As noted several times in previous chapters, the ITAU has targeted a very broad set of services in the Russian society. However, targets such as hospitals have been avoided and even discouraged – even questions related to attacking hospitals are responded by the other volunteers that those should not be targeted. Also, one clear "boundary case" is the targeting of pension funds as seen in Figure 18. This case resonated discussion and commenting on the ethicality of the targets, where some argued that conducting DDoS is nothing in comparison to Russians bombing civilians – while some raised up that this might directly affect children and elderly that do not even have any family members fighting in the war.


IT ARMY of Ukraine
Меню
Пенсионный фонд Российской Федерации
En
AA
Выберите свой регион
Главная / Гражданам / Меры поддержки, переданные из органов... / Семьям военных и сотрудников силовых в...

Семьям военных и сотрудников силовых ведомств

Компенсация коммунальных платежей

Единовременная выплата на ремонт дома

Ежегодная выплата на летний оздоровительный отдых ребенка

Ежемесячное пособие детям военнослужащих

Ежемесячная компенсация инвалидам вследствие военной травмы и членам семьи погибшего (умершего) военнослужащего

Сьогоднішня ціль це пенсійний фонд рф. Чому? Тому що через нього сім'ї військових отримують виплати та компенсації.

—

Today's target is the pension fund of the russian federation. Why? Because through it, russian military families receive payments and compensation.

Figure 18 Targetting Pension-funds

As articulated by Pondy and Mitroff (1979, p. 7), an open system shows no more variety than its environment exposes it to; similar concept can be drawn from the case of ITAU. While not saying that this is the case mathematically, it is so at least in the metaphorically, which is one of the school of thought in complexity science (Raisio & Lundström, 2017). While ITAU has variety in individual capabilities that are perceived among its ranks, from very technical people to non-technical, from very active and seemingly motivated to those who primarily lurk and contribution ambiguous and to the used tools, tactics, procedures, and ways of communication – these are items that are found it its environment. However, it is more arguable, that it is the more emergent properties that make the ITAU stand out from its environment, and not necessarily its variety.

5.10 Concluding note on the theoretical lens

Utilizing the Complex Adaptive Systems theory as a theoretical lens for the study of the IT Army of Ukraine proved to be both challenging and rewarding thorough the study-process. As a theoretical lens, CAS has a wide and substantial literature to back on (Preiser et al., 2018), especially from the broader Complexity Sciences perspective. However, as an applicable "off-the-shelf" analytical lens it still lacks rigor, mostly due to the fact that in the context of softer sciences the concepts have inherent ambiguity and interpretability (Raisio & Lundström, 2017).

From the perspective of the researcher, CAS offers metaphorically strong set of concepts that can provide valuable tools for thought in seeing patterns when studying complex phenomena, as has been the case in this study. While "forcing" observations and elements of a complex system under labels to enable the coherence of a written report can be challenging and feel counter-intuitive, it is nevertheless a challenge that sometimes needs to be solved both during the analysis and reporting phase of a study.

6 CONCLUSION

This thesis embarked on a mission to study an organization set in at a what can be best described as unique context, post-1945 large-scale warfare in Europe. While cyber-operations in European context (Estonia) and activities resembling cyberwarfare during the Georgian conflict bring notable similarities to current state of affairs, it should be noted that the cyberwarfare that has accompanied the Russo-Ukrainian war is on a level unseen in previous conflicts. Organizations operating in the cyber-domain in general are not considered to be very open for research, nor participation, and here an opportunity presented itself for the researcher that was capitalized upon.

Since the organization and the context that it resided in was immediately seen to be very complex in nature to the researcher, it was decided to use a theoretical lens appropriate for such context. Emerging from the domain of complexity science, the concept of Complex Adaptive Systems (Holland, 2012; Levin, 2002) was seen as a suitable lens to use with its extensive background literature (Preiser et al., 2018) and application to the study of organizations. These principles served as the core on answering the research question (RQ1) of *What are the characteristics of CAS that can be found in ITAU?*

From the broad set of theoretical and conceptual background literature, relevant principles were aggregated in order to provide structure for the analysis of the ITAU as a Complex Adaptive System. These principles were Adaptation/Homeostasis, Nonlinearity, Emergence, Self-organization, Feedback, Diversity/Individuality, Cooperation/Communication, Co-evolution, and Openness/Contextuality (Anderson, 1999; Arthur, 1988; Buckley, 1968; Cilliers, 1998; Holland, 1995; Lewin, 1999). The IT Army of Ukraine most strongly represented a Complex Adaptive System by continuously adapting in response to its environment and changing circumstances such as numbers of followers and technical sophistication.

However, on occasion it not only adapted but co-evolved in connection with its target system – the Russian society – which mostly represented itself in hardening the targets of DDoS attacks. The ability to self-organize became the backbone of learning and utilization of diverse tools for conducting its daily operations, but also in diverging into subgroups. This self-organization on the other hand would not have emerged without the inherent openness and open communication it had, having also their attacks having expanded in nonlinear ways by being shared in other DDoS groups. And jumping back to adaptation and co-evolution, the fact that ITAU had its radical openness through Telegram and target listing, meant that it had to shift into closed listing of targets in order to continue successfully operating.

To gain insights into the ITAU, a qualitative methodology was needed in order to gain insights into the principles of CAS mentioned previously. However, the context of study could be said to be sensitive to the very least, even with the group seemingly being radically open. Thus, the methodological approach of ethnography-oriented case study (Côté-Boileau et al., 2020) was taken. Ethnography is even seen necessary for studying CAS in the sense of organizations (Güney, 2010), and for this context especially the ethnography in the virtual sense (Hine, 2000) was clearly the only viable way for the researcher to bite into the organization of ITAU. The study lasted from February 2022 to May 2023, with the duration of approximately 15 months.

Future research that would extend the research conducted in this thesis could include in-depth studies on the experiences of the volunteers of ITAU, and also extend to those that have been in the "invisible side" of the organization – preferably even those that have been part of the decision-making processes of the group. The first one would bring more insights into the impact of changes that the group has evolved through from the perspective of the volunteer who have lived through it. The second could bring light into the actual reasons and realities why the group has changed as it has – as an example, what role has the environment such as target hardening had in the change of tactics, versus possible internal metrics such as participation rate of volunteers?

This thesis contributes to the existing literature on Cyberwarfare in two significant ways: First, it adds to the contemporary subject of Cyberwarfare and brings detailed insights into the activities and properties of the IT Army of Ukraine. Second, it introduces the theoretical concept of Complex Adaptive Systems (CAS) as a valuable analytical tool for studying cyber groups. From a Complexity Sciences perspective, this thesis extends the application of CAS theory to the context of Cyber groups and Cyberwarfare, areas that have been relatively underexplored from this standpoint. This thesis can also bring insights for the practitioners in the Cyber-domain to support analysis of similar types of groups and phenomena, of which could be more common in the future.

REFERENCES

Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security*, *86*, 402–418. https://doi.org/10.1016/j.cose.2019.07.001

Anderson, P. (1999). Complexity Theory and Organization Science. *Organization Science*, 216–232.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the Cost of Cybercrime. In R. Böhme (Ed.), *The Economics of Information Security and Privacy* (pp. 265–300). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39498-0_12

Andress, J., & Winterfeld, S. (2014). *Cyber warfare: Techniques, tactics and tools for security practitioners* (Second edition). Elsevier.

Ankel, S. (2022). *100 drafted Russian soldiers went on strike, refusing to fight in Ukraine after not getting paid, report says.* https://www.businessinsider.com/drafted-russia-soldiers-on-strike-after-not-getting-paid-report-2022-11?r=US&IR=T

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, *12*(2), 141–165. https://doi.org/10.1080/01495939308402915

Arthur, W. B. (1988). Self-reinforcing mechanisms in economics. In P. Anderson, K. Arrow, & D. Pines (Eds.), *The economy as an evolving complex system* (pp. 9–31). Addison Wesley.

Behzadan, V., & Munir, A. (2017). *Models and Framework for Adversarial Attacks on Complex Adaptive Systems* (arXiv:1709.04137). arXiv. http://arxiv.org/abs/1709.04137

Björk, P., & Kauppinen-Räisänen, H. (2012). A netnographic examination of travelers' online discussions of risks. *Tourism Management Perspectives*, *2*(3), 65–71. https://doi.org/10.1016/j.tmp.2012.03.003

Boisot, M., & Child, J. (1999). Organizations as Adaptive Systems in Complex Environments: The Case of China. *Organization Science*, *10*(3), 237–252. https://doi.org/10.1287/orsc.10.3.237

Brewer, J. (2000). *Ethnography*. Buckingham: Open University Press.

Buckley, W. (1968). Society as a Complex Adaptive Systems. In *Systems Research for Behavioral Science – A Sourcebook* (pp. 490–513). Routledge.

Burita, L., & Le, D. T. (2021). Cyber Security and APT Groups. *2021 Communication and Information Technologies (KIT)*, 1–7. https://doi.org/10.1109/KIT52904.2021.9583744

Carlisle, Y., & McMillan, E. (2006). INNOVATION IN ORGANIZATIONS FROM A COMPLEX ADAPTIVE SYSTEMS PERSPECTIVE. *Emergence: Complexity and Organizations*, *8*(1), 2–9.

Cilliers, P. (1998). *Complexity & Postmodernism – Understanding complex systems*. Taylor & Francis.

Cilliers, P. (2001). Boundaries, Hierarchies and Networks in Complex Systems. *International Journal of Innovation Management*, *5*(2), 135–147.

Cilliers, P., & Spurrett, D. (1999). Complexity and post-modernism: Understanding complex systems. *South African Journal of Philosophy*, *18*(2), 258–274. https://doi.org/10.1080/02580136.1999.10878187

Clarke, R., & Knaape, R. (2011). *Cyber war: The next threat to national security and what to do about it*. Harper-Collins.

Cole, B. (2023). Russian Troops Fighting "for free" as Pay Is Delayed for Months. *Newsweek*. https://www.newsweek.com/russia-ukraine-putin-free-payments-1789846

Cooper, J., & Harrison, D. (2001). The social organization of audio piracy on the Internet. *Media, Culture & Society*, *23*(1), 71–89. https://doi.org/10.1177/016344301023001004

Côté-Boileau, E., Gaboury, I., Breton, M., & Jean-Louis, D. (2020). Organizational Ethnographic Case Studies: Toward a New Generative In-Depth Qualitative Methodology for Health Care Research? *International Journal of Qualitative Methods*, *19*, 1–17. https://doi.org/10.1177/1609406920926904

Creswell, J. W., & Miller, D. L. (2000). Determining Validity in Qualitative Inquiry. *Theory Into Practice*, *39*(3), 124–130. https://doi.org/10.1207/s15430421tip3903_2

da Cruz, J. de A., & Pedron, S. (2020). Cyber Mercenaries: A New Threat to National Security. *International Social Science Review*, *96*(2).

Dave, P., & Dastin, J. (2022). Exclusive: Ukraine has started using Clearview AI's facial recognition during war. *Reuters*. https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/

Denzin, N., & Lincoln, Y. (2017). *The SAGE Handbook of Qualitative Research* (5th ed.).

Deseriis, M. (2017). Hacktivism: On the Use of Botnets in Cyberattacks. *Theory, Culture & Society*, *34*(4), 131–152. https://doi.org/10.1177/0263276416667198

Disbalancer. (2022). How to Download Liberator? *Disbalancer Website*. https://disbalancer.com/download/

Domíniquez, D., Beaulie, A., Estalella, A., & Gómez, E. (2007). Virtual Ethnography. *Qualitative Social Research*, *8*(3).

Dooley, K. J. (1997). A Complex Adaptive Systems Model of Organization Change. *Nonlinear Dynamics, Psychology, and Life Sciences*, *1*(1), 59–97.

Driscoll, C., & Gregg, M. (2010). My profile: The ethics of virtual ethnography. *Emotion, Space and Society*, *3*(1), 15–20. https://doi.org/10.1016/j.emospa.2010.01.012

Easton, D. (1968). A Systems Analysis of Political Life. In W. Buckley (Ed.), *Systems Research for Behavioral Science – A Sourcebook*. Taylor & Francis.

Ebo, B. (1998). Internet or Outernet? In *Cyberghetto or Cybertopia? Race, Class, and Genger on the Internet.* (pp. 1–12). Praeger.

Estonian Defence League. (2023a). Estonian Defence League's Cyber Unit. *Kaitseliit*. https://www.kaitseliit.ee/en/cyber-unit

Estonian Defence League. (2023b). History of the EDL CU. *Kaitseliit*. https://www.kaitseliit.ee/en/history-of-the-edl-cu

Fekolkin, R. (2015). *CAS and Game Theory in Critical Infrastructure:*

Ferretti, M., Richards, T., Irons, J., & Richards, K. (2022). The Dimensionality of the Cyber Warrior. *HCII 2022, LNCS 13333*, 326–339. https://doi.org/10.1007/978-3-031-05563-8_21

Fields, D., & Kafai, Y. (2009). A connective ethnography of peer knowledge sharing and diffusion in a tween virtual world. *Computer-Supported Learning*, *4*(1), 47–68.

Filotas, E., Parrott, L., Burton, P. J., Chazdon, R. L., Coates, K. D., Coll, L., Haeussler, S., Martin, K., Nocentini, S., Puettmann, K. J., Putz, F. E., Simard, S. W., & Messier, C. (2014). Viewing forests through the lens of complex systems science. *Ecosphere*, *5*(1), art1. https://doi.org/10.1890/ES13-00182.1

Flick, U. (2018a). Triangulation. In N. Denzin & Y. Lincoln (Eds.), *Sage handbook of qualitative research*. Sage.

Flick, U. (2018b). Triangulation in ethnography. In *Doing triangulation and mixed methods* (pp. 49–70). SAGE Publications Ltd. https://dx.doi.org/10.4135/9781529716634

Frankel, M., & Siang, S. (1999). Ethical and legal aspects of human subjects on the internet. *American Association for the Advancement of Science WOrkshop Report*, 18.

Gable, K. (2010). Cyber-apocalypse now: Securing the internet against cyberterrorism and using universal jurisdiction as a deterrent. *Vanderbilt Journal of Transnational Law*, *43*(1), 57–118.

GDC. (2022). Hackers Hacked United Aircraft Corporation Website. *Global Defence Corp*. https://www.globaldefensecorp.com/2022/04/18/hackers-hacked-united-aircraft-corporation-website/

Gear, C., Eppel, E., & Koziol-Mclain, J. (2018). Advancing Complexity Theory as a Qualitative Research Methodology. *International Journal of Qualitative Methods*, *17*(1), 160940691878255. https://doi.org/10.1177/1609406918782557

Golafshani, N. (2003). Understanding Reliability and Validity in Qualitative Research. *The Qualitative Report*, *8*(4), 597–606. https://doi.org/10.46743/2160-3715/2003.1870

Gordon, S., & Ford, R. (2002). Cyberterrorism? *Computers & Security*, *21*(7), 636–647.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

Grisogono, A.-M. (2006). The Implications of Complex Adaptive Systems Theory for C2. *CCRTS 2006*.

Güney, S. (2010). New Significance for an Old Method: CAS Theory and Ethnography. *Communication Methods and Measures*, *4*(3), 273–289. https://doi.org/10.1080/19312458.210.505499

Gureckis, T., & Goldstone, R. (2006). Thinking in groups. *Pragmatics & Cognition*, *14*(2), 293–311.

Harrison Dinniss, H. (2012). *Cyber Warfare and the Laws of War*.

Hewson, C. (2003). *Internet research methods: A practical guide for the social and behavioural sciences*. Sage Publications.

Hildreth, S. (2001). *Cyberwarfare*. Congressional Research Service, Report for Congress. https://irp.fas.org/crs/RL30735.pdf

Hine, C. (2000). *Virtual ethnography*. https://doi.org/10.4135/9780857020277

Hollan, J., Hutchins, E., & Kirsh, D. (2000). Distributed cognition: Toward a new foundation for human-computer interaction research. *ACM Transactions on Computer-Human Interaction*, *7*(2), 174–196. https://doi.org/10.1145/353485.353487

Holland, J. (1995). *Hidden Order: How adaptation builds complexity.* Addison Wesley.

Holland, J. H. (2012). *Signals and Boundaries: Building Blocks for Complex Adaptive Systems*. The MIT Press. https://doi.org/10.7551/mitpress/9412.001.0001

Holt, T., & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies*, *23*(1), 33–50. https://doi.org/10.1080/14786011003634415

Hua, J., Chen, Y., & Luo, X. (Robert). (2018). Are we ready for cyberterrorist attacks?—Examining the role of individual resilience. *Information & Management*, *55*(7), 928–938. https://doi.org/10.1016/j.im.2018.04.008

Hughes, D., & Colarik, A. (2017). The Hierarchy of Cyber War Definitions. In G. A. Wang, M. Chau, & H. Chen (Eds.), *Intelligence and Security Informatics* (Vol. 10241, pp. 15–33). Springer International Publishing. https://doi.org/10.1007/978-3-319-57463-9_2

Hunker, J. (2010). Cyber war and cyber power. *Issues for NATO Doctrine*, *62*. https://www.files.ethz.ch/isn/124343/rp_62.pdf

Hutchins, E. (1995). *Cognition in the Wild*. The MIT Press.

Hutchins, E., & Klausen, T. (1996). Distributed cognition in an airline cockpit. In Y. Engeström & D. Middleton (Eds.), *Cognition and Communication at Work* (1st ed., pp. 15–34). Cambridge University Press. https://doi.org/10.1017/CBO9781139174077.002

Hutchinson, W. (2021). Some basic principles of Information Warfare. *Journal of Information Warfare*, *20*(4), 1–6.

Hutchinson, W., & Warren, M. (2001). Principles of Information Warfare. *Journal of Information Warfare*, *1*(1), 1–6.

Ireton, C., & Posetti, J. (2018). *Journalism, Fake news & Disinformation: Handbook for Journalism Education and Training*. UNESCO Publishing.

Jithesh, A. (2020). Disinformation as a strategic weapon: Roles of societal polarization, government's cybersecurity capability, and the rule of law. *ICIS 2020 Proceedings*, *12*.

Johnson, C. W. (2014). Anti-social networking: Crowdsourcing and the cyber defence of national critical infrastructures. *Ergonomics*, *57*(3), 419–433. https://doi.org/10.1080/00140139.2013.812749

Kauffman, S. (1996). *At Home in the Universe: The Search for the Laws of Self-Organization and Complexity*. https://www.jstor.org/stable/1576330?origin=crossref

Korns, S. W., & Kastenberg, J. E. (2008). Georgia's Cyber Left Hook. *The US Army War College Quarterly: Parameters*, *38*(4). https://doi.org/10.55540/0031-1723.2455

Kozinets, R. (2002). The Field Behind the Screen: Using Netnography for Marketing Research in Online Communities. *Journal of Marketing Reserach*, *39*(1), 61–72. https://doi.org/10.1509/jmkr.39.1.61.18935

Kozinets, R. (2010). *Netnography: Doing Ethnographic Research Online*. London: Sage.

Ladyman, J., Lambert, J., & Wiesner, K. (1993). What is a Complex System? *European Journal for Philosophy of Science*, *3*(1), 33–67. https://doi.org/10.1007/s13194-012-0056-8

Langer, R., & Beckman, S. C. (2005). Sensitive research topics: Netnography revisited. *Qualitative Market Research: An International Journal*, *8*(2), 189–203. https://doi.org/10.1108/13522750510592454

Lehto, M., & Henselmann, G. (2020). *Non-Kinetic Warfare: The New Game Changer in the Battle Space*. International Conference on Cyber Warfare and Security.

Lemay, A., Calvet, J., Menet, F., & Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. *Computers & Security*, *72*, 26–59. https://doi.org/10.1016/j.cose.2017.08.005

Levin, S. (1999). *Fragile dominion: Complexity and the commons*. Perseus Books.

Levin, S. (2002). Complex adaptive systems: Exploring the known, the unknown and the unknowable. *Bulletin of the American Mathematical Society*, *40*(1), 3–19. https://doi.org/10.1090/S0273-0979-02-00965-5

Levitt, H., Bamberg, M., Creswell, J., Josselson, R., Frost, D., & Suárez-Oronco, C. (2018). Journal Article Reporting Standards for Qualitative Primary, Qualitative Meta-Analytic, and Mixed Methods Research in Psychology: The APA Publications and Communications Board Task Force Report. *Americal Psychologist*, *73*(1), 26–46. https://doi.org/10.1037/amp0000151

Lewin, R. (1999). *Complexity – Life at the Edge of Chaos*.

Lockheed Martin. (2023). The Cyber Kill Chain. *Lockheed Martin Official Homepage*. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Lorentz, E. (1972). *Predictability: Does the flap of a butterly's wings in Brazil set off a Tornado in Texas.* American Association for the Advancement of Science. https://eapsweb.mit.edu/sites/default/files/Butterfly_1972.pdf

Lucas, G. (2014). State-Sponsored Hackivism and the Rise of “Soft” War. *Soft War*, 77–87. https://doi.org/10.1017/S1355770X12000460

Luoma, M., & Lindell, J. (2020). Johtaminen ja Kompleksisuus—Kolmijaosta Kokonaisvaikutukseen. In *Johtaminen kompleksisesssa maailmassa* (1st ed.). Gaudeamus.

Marion, R., & Uhl-Bien, M. (2001). Leadership in complex organizations. *The Leadership Quarterly*, *12*(4), 389–418. https://doi.org/10.1016/S1048-9843(01)00092-3

Marti, C. (2018). *Armies as complex adaptive systems*.

Maurer, T. (2018). Cyber Mercenaries—The State, Hackers, and Power. *Cambridge University Press*, 268. https://doi.org/10.1017/9781316422724

McDaniel, R. R., & Driebe, D. J. (2001). Complexity science and health care management. In *Advances in Health Care Management* (Vol. 2, pp. 11–36). Emerald (MCB UP). https://doi.org/10.1016/S1474-8231(01)02021-3

McDaniel, R. R., Lanham, H. J., & Anderson, R. A. (2009). Implications of complex adaptive systems theory for the design of research on health care organizations. *Health Care Management Review*, *34*(2), 191–199. https://doi.org/10.1097/HMR.0b013e31819c8b38

McReynolds, P. (2015). How to Think About Cyber Conflicts Involving Non-state Actors. *Philosophy & Technology*, *28*(3), 427–448. https://doi.org/10.1007/s13347-015-0187-x

Merali, Y., & Allen, P. (2011). Complexity and Systems thinking. In P. Allen, S. Maguire, & B. McKelvey, *The Sage Handbook of Complexity and Management* (pp. 1–26). SAGE Publications Ltd. https://doi.org/10.4135/9781446201084.n1

Merilehto, J. (2022). Inter-Team Cognitive Diversity – Using Distributed Cognition for Analyzing Team Cognitive Diversity. *Proceedings of the 44th Annual Conference of the Cognitive Science Society*, *44*. https://escholarship.org/uc/item/1t6666t6

Merilehto, J., & Riihikoski, R. (2022). *HYBRID WORK THROUGH THE LENS OF DISTRIBUTED COGNITION – CASE GOFORE OYJ* [University of Jyväskylä]. https://jyx.jyu.fi/handle/123456789/81824

Milno, D. (2022). Amateur hackers warned against joining Ukraine’s ‘IT army.’ *The Guardian*. https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army

Mkono, M. (2011). The Othering of Food in Touristic Eatertaintment: A Nernograpgy. *Tourist Studies*, *11*(3), 253–270.

Morse, J. (2017). Refreming Rigor in Qualitative Inquiry. In *Handbook of Qualitative Research* (5th ed., pp. 1373–1409). Sage.

Murthy, D. (2008). Digital ethnography: An examination of the use of new technologies for social research. *Sociology*, *42*(5), 837–855.

Mykhailo, F. (2022, January 19). *[@FedorovMykhailo]. (2022, January 19). We are creating an IT army. All operational tasks will be given here [Tweet]. Twitter.* [Tweet]. Twitter. https://twitter.com/FedorovMykhailo/status/1497642156076511233

Narula, S. (2004). Psychological operations (PSYOPs): A conceptual overview. *Strategic Analysis*, *28*(1), 177–192. https://doi.org/10.1080/09700160408450124

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. *Computers & Security*, *31*(4), 418–436. https://doi.org/10.1016/j.cose.2012.02.009

Nye, Jr. J. (2011). *Nuclear Lessons for Cyber Security:* Defense Technical Information Center. https://doi.org/10.21236/ADA553620

Perry, M. (2010). Socially distributed cognition in loosely coupled systems. *AI & SOCIETY*, *25*(4), 387–400. https://doi.org/10.1007/s00146-010-0267-5

Pondy, L., & Mitroff, I. (1979). Beyong Open System Models of Organization. *Research in Organizational Behavior*, *1*, 3–39.

Povaliaieva, O. (2022). Ukrainian IT Army Hacked Russia. *Good Time Invest*. https://good-time-invest.com/blog/ukrainian-it-army-hacked-russia/

Preiser, R., Biggs, R., De Vos, A., & Folke, C. (2018). Social-ecological systems as complex adaptive systems: Organizing principles for advancing research methods and approaches. *Ecology and Society*, *23*(4), art46. https://doi.org/10.5751/ES-10558-230446

Puri, A. (2007). The Web of Insights: The Art and Practice of Webnography. *International Journal of Market Research*, *49*(3), 387–408. https://doi.org/10.1177/147078530704900308

Puusa, A., & Juuti, P. (2020). *Laadullisen tutkimuksen näkökulmat ja menetelmät*. Gaudeamus.

Raisio, H., & Lundström, N. (2017). Managing Chaos: Lessons From Movies on Chaos Theory. *Administration & Society*, *49*(2), 296–315. https://doi.org/10.1177/0095399714541269

RAND Corporation. (2023). Cyber Warfare. *Cyber Warfare*. https://www.rand.org/topics/cyber-warfare.html

Reuters. (2022). Website of Russian oil firm Gazprom Neft goes down after apparent hack. *Reuters*. https://www.reuters.com/business/energy/russian-oil-company-gazprom-nefts-website-appears-have-been-hacked-2022-04-06/

Richards, I., & Wood, M. A. (2018). *Hacktivists Against Terrorism: A Cultural Criminological Analysis Of Anonymous' Anti-Is Campaigns*. https://doi.org/10.5281/ZENODO.1467895

Richardson, K. A. (2008). *Managing Complex Organizations: Complexity Thinking and the Science and Art of Management*. *10*(2).

Richardson, K., & Cilliers, P. (2001). What is Complexity Science? A view from different directions. *Emergence: Complexity and Organizations*, *3*(1), 5–23.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2018). An introduction to cyber peacekeeping. *Journal of Network and Computer Applications*, *114*, 70–87. https://doi.org/10.1016/j.jnca.2018.04.010

Roundy, P. T., Bradshaw, M., & Brockman, B. K. (2018). The emergence of entrepreneurial ecosystems: A complex adaptive systems approach. *Journal of Business Research*, *86*, 1–10. https://doi.org/10.1016/j.jbusres.2018.01.032

Rybas, N., & Gajjala, R. (2007). Developing Cyberethnographic Research Methods for Understanding Digitally Mediated Identities. *Qualitative Social Research*, *8*(3), 1–33.

Schaap, A. (2009). Cyber Warfare Operations: Development and use under international law. *The Air Force Law Review*, *64*, 121–173.

Schmitt, M. (2012). Classification of Cyber Conflict. *Journal of Conflict and Security Law*, *17*(2), 245–260. https://doi.org/10.1093/jcsl/krs018

Schneider, M., & Somers, M. (2006). Organizations as complex adaptive systems: Implications of Complexity Theory for leadership research. *The Leadership Quarterly*, *17*(4), 351–365. https://doi.org/10.1016/j.leaqua.2006.04.006

Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to cyber-warfare: A multidisciplinary approach*. Syngress.

Simon, H. (1997). *Model of Bounded Rationality*. The MIT Press.

Stacey, R. D. (1995). The science of complexity: An alternative perspective for strategic change processes. *Strategic Management Journal*, *16*(6), 477–495. https://doi.org/10.1002/smj.4250160606

Stacey, R. D. (1996). *Complexity and creativity in organizations* (1st ed). Berrett-Koehler Publishers.

Starbird, K., Wilson, T., & Arif, A. (2019). Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), 1–26. https://doi.org/10.1145/3359229

Sugiura, L., Wiles, R., & Pope, C. (2017). Ethical challenges in online research: Public/private perceptions. *Research Ethics*, *13*(3–4), 184–199. https://doi.org/10.1177/1747016116650720

Svyrydenko, D., & Mozgin, W. (2022). Hacktivism of the Anonymous Group as a Fighting Tool in the Context of Russia's War against Ukraine. *Future Human Image*, *17*. https://doi.org/10.29202/fhi/17/6

TGStat. (n.d.). IT Army of Ukraine. *TGStat*. https://tgstat.com/channel/@itarmyofukraine2022/stat/subscribers

Thrift, N. (1999). The Place of Complexity. *Theory, Culture & Society*, *16*(3), 31–69. https://doi.org/10.1177/2F02632769922050610

Toulas, B. (2022). Malware disquised as security tool targets Ukraine's IT Army. *BleepingComputer*. https://www.bleepingcomputer.com/news/security/malware-disguised-as-security-tool-targets-ukraines-it-army/

Uhl-Bien, M., & Marion, R. (2009). Complexity leadership in bureaucratic forms of organizing: A meso model. *The Leadership Quarterly*, *20*(4), 631–650.

UN News. (2022, February 3). General Assembly resolution demands end to Russian offensive in Ukraine. *UN News*. https://news.un.org/en/story/2022/03/1113152

Vegh, S. (2002). Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking. *First Monday*, *7*(10). https://doi.org/10.5210/fm.v7i10.998

von Bertalanffy, L. (1950). The Theory of Open Systems in Physics and Biology. *Science*, *111*(2872), 23–29. https://doi.org/10.1126/science.111.2872.23

von Bertalanffy, L. (1962). General Systems Theory—A Critical Review. *General Systems*, *VII*, 1–20.

Wallenius, C. (2022). Do Hostile Information Operations Really Have the Intended Effects? A Literature Review. *Journal of Information Warfare*, *21*(2), 21–25.

Ward, K. (1999). The Cyber-Ethnographic (Re)Construction of Two Feminist Online Communities. *Sociological Research Online*, *4*(1), 51–64. https://doi.org/10.5153/sro.222

Waterman, S. (2023). Ukraine Scrambles to Draft Cyber Law, Legalizing Its Volunteer Hacker Army. *Newsweek*. https://www.newsweek.com/ukraine-drafting-new-law-legalizing-volunteer-hacker-cyber-army-red-cross-1786814

Webber, C., & Yip, M. (2018). *The Rise Of Chinese Cyber Warriors: Towards A Theoretical Model Of Online Hacktivism*. https://doi.org/10.5281/ZENODO.1467901

Wesch, M. (2009). Youtube and you—Experience of self-awareness in the context of collapse of the recording webcam. *Explorations in Media Technology*, *8*(2), 19–34.

Wu, L., Morstatter, F., Carley, K. M., & Liu, H. (2019). Misinformation in Social Media: Definition, Manipulation, and Detection. *ACM SIGKDD Explorations Newsletter*, *21*(2), 80–90. https://doi.org/10.1145/3373464.3373475

Yale School of Management. (2023). *Over 1,000 Companies Have Curtailed Operations in Russia—But Some Remain*. https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain

Yin, R. (2018). *Case Study Research and Applications: Design and Methods* (6th ed.). Thousand Oaks, CA: Sage.

Zotov, A. (2022). Cyberattack Knocks Out Russian Video Platform Rutube. *The Moscow Times*. https://www.themoscowtimes.com/2022/05/09/ukrainians-being-taken-against-their-will-into-russia-pentagon-a77628