

Institut Barcelona d'Estudis Internacionals

Academic Years 2021 – 2023



Co-funded by the  
Erasmus+ Programme  
of the European Union



Non-state actors in Cyberconflict

Explaining the involvement of KillNet hacker collective in the Russia-Ukraine  
Conflict

Dissertation submitted by

Cristina Ciobotariu

in partial fulfilment of the requirements for the degree of  
ERASMUS MUNDUS MASTER'S PROGRAMME IN PUBLIC POLICY (MMAPP)

Supervisor: Cameran Ashraf & Josep Ibáñez

Barcelona, July, 2023

# TABLE OF CONTENTS

<b>1. Introduction .....</b>	<b>1</b>
<b>2. Hackers, hacktivism and geopolitics: the process of shaping the cyberspace .....</b>	<b>4</b>
2.1. Conceptual note: Clarifying the definition of Hacktivism .....	4
2.2. The construction of cyberspace geopolitics .....	5
2.3. Non-State Actors in Cyberspace .....	7
2.4. Constructivism and Actor Network Theory for connecting the social and material of political hacking.....	9
2.5. Idea, identity, and collectivity: Intersubjective reality of politically motivated hacking .....	10
<b>3. The birth of Russian Hacktivism: the case study of KillNet .....</b>	<b>14</b>
3.1. Background information .....	14
3.2. Killnet general overview .....	16
3.3. Organisation .....	17
3.4. Tactics and Instruments .....	20
3.5. Communication and public engagement strategy .....	22
3.6. Collective Identity .....	25
<b>4. Understanding the future role of Hactivism .....</b>	<b>27</b>
4.1. The hacker and the bot: Killnet's socio-technical network is shaping their identity and discourse .....	27
4.2. Killnet changed the way hacktivism is to be understood .....	29
4.3. Killnet is an idea and a brand: why attention matters .....	30
4.4. The future of the hacker and the state .....	32
<b>5. Conclusions .....</b>	<b>34</b>
<b>6. Bibliography .....</b>	<b>36</b>
<b>Annex .....</b>	<b>v</b>

## **List of Abbreviations**

ANT – Actor-Network Theory

CIS - Common wealth of Independent states

Dos/Ddos - Denial-of-Service/Distributed Denial-of-Service

EIB – Europan Investment Bank

ER – Engagement rate#

FSB – Federal Security Service

GRU – Russian General Staff Main Intelligence Directorate

ICTs – Information and communication technologies

IOs – International Organisations

NSA/s – Non-state Actor/s

OSINT – Open Source Intelligence

PR – Public Realtions

## ABSTRACT

The hybrid nature of Russia's invasion of Ukraine has drawn the attention of various cybercrime and hacktivist groups into the conflict. Among these groups, Killnet emerged as a significant player, aligning itself with the Russian government and targeting actors supporting Ukraine. As the involvement of hacker collectives becomes a critical dimension in inter-state conflicts, this thesis seeks to unravel the motivations and actions of Killnet, shedding light on the subjective and objective aspects of hacktivism. Using qualitative analysis, this research delves into Killnet's identity, motivations, activities, organization, tactics and communication processes to comprehend how and why hackers engage in interstate conflicts. The study employs constructivist lenses and actor-network theory logic alongside social media analysis for exploring the role of ideas, norms, and social and material interactions that influence hackers' political agendas. The case study highlights the importance of nationalism and hacker culture in explaining hackers' involvement in international conflicts. Intersubjective meanings are attributed to hacktivism by socio-technical networks, meanings that strengthen the phenomenon of non-state actors in cyberspace. These meanings further shape and construct realities in cyberspace and conflict surrounding it.

**Keywords:** Hacktivism, Killnet, Constructivism, hacker, cyberconflict, intersubjectivity, cyberspace

## 1. Introduction

The hybrid nature of Russia's invasion of Ukraine facilitated the involvement of many cybercrime and hacktivist groups in the conflict (Przetacznik & Tarpova, 2022; Svyrydenko & Mozgin, 2022; Yildirim, 2022). Shortly after the Russian invasion of Ukraine started, Anonymous<sup>1</sup>, Conti<sup>2</sup>, KillNet<sup>3</sup>, and other hacker groups picked sides (Yildirim, 2022). In March 2022, major intelligence agencies alerted about the rise of cyber threats and cybercrime in the context of this conflict, with cyberattacks that will target actors beyond the two belligerent countries (CISA, 2022). By December 2022, the industry reported that approximately 190 groups on both sides declared intent to be involved in the conflict between Russia and Ukraine (Yildirim, 2022). This conflict became an ongoing experimentation of the evolving phenomenon of hacker collectives' involvement in an inter-state war.

The phenomenon of non-state actors (NSAs) pursuing political motivations using information and communication tools has been introduced previously (Abrahamsen & Williams, 2009; Bussolati, 2015; Denning, 2001). Previous analysis of NSAs conducting cyberattacks found two main motivations that sometimes can be intertwined: financial and political (Bussolati, 2015; Maurer, 2018, p. 152; Valeriano & Maness, 2015). Financial motivations were pursued by creating cybercriminal organisations that would offer hack-for-hire services or be used as cyber proxies by states (Bussolati, 2015, p. 109; Dumbrava, 2012; Maurer, 2018). On the other hand, political motivations were highlighted by cyberattacks conducted in the name of internet freedom, information liberalisation, patriotism or other political ideologies and beliefs.

In February 2022, the hacker collective KillNet became public as a group aligned with the Russian government and started attacking actors supporting Ukraine. Compared with other hacker groups notorious for committing cybercrimes before the invasion of Ukraine, KillNet's existence was unindexed on the web until the beginning of the conflict. The first official mention of KillNet was in May 2022 in the CISA (2022) report of Five Eyes, an extensive alert on State and Non-state threat actors on the Russian side. On the opposite side, the most known hacker collective on the

---

<sup>1</sup> Anonymous is the most known hacker collective, active since 2003.

<sup>2</sup> Conti, also known as Wizard Spider, is a less popular cybercrime group that conducted politically driven destructive cyberattacks against Costa Rica, which led to the state declaring a state of emergency, see more (CISA, 2022; "Rodrigo Chaves sobre ciberataques," 2022)

<sup>3</sup> KillNet is a Russian ideologically aligned hacker group that made its existence widely public at the start of the 2022 Russian invasion of Ukraine

international stage, Anonymous, declared “cyberwar to Russia” (Milmo & editor, 2022). The question that follows this empirical situation is how and why these individuals come together to pursue a political agenda on the international stage through the use of cyberattacks and other digital instruments.

This study employs a combined approach, integrating a constructivist historical account with a qualitative analysis, to comprehensively examine the evolution and dynamics of the hacker collective Killnet to understand how and why they got involved in interstate conflict. Moreover, I looked at the group through not only through constructivist lenses (Branch, 2018; Hurd, 2008; Reardon & Choucri, 2012; Wendt, 1992) but also actor-network theory (ANT) logic (Cresswell et al., 2010; Jóhannesson & Bærenholdt, 2009; Luppicini, n.d.) examining how ideas, norms, and social and material interactions influence political hacking activities and acknowledging that hacker collectives are “black boxes” composed of equally relevant human and non-human elements. With the added complexity to the international stage posed by the emerging political involvement of hackers (Denning, 2001; Hardy, 2010; Ireland, 2022; Li, 2013) and the hybrid nature of the future inter-state conflicts (Atrews, 2020; Bussolati, 2015; Leuprecht et al., 2019), it is of high relevance to shed light on how these individuals narrate their way into cyberconflicts. Understanding KillNet’s involvement and motivations is highly relevant, mainly due to the group’s creation in the context of the Russian invasion of Ukraine and its exponential popularity.

Exploring KillNet’s black box not only enables a deeper comprehension of the subjective aspects of the puzzle but also provides valuable insights into the behind-the-scenes process of hacktivism. Examining their activities, organisation, structure and techniques will provide an answer to the “how?” question. Meanwhile, understanding the subjective part of their activities sheds light on the reasons for conducting hacktivism, addressing the “why?” aspect of the research question. While the findings of this study might not explain thoroughly all forms of political hacking, it will shed light, especially on Russian patriotic hacking. The thesis is divided into four parts. In the first part, I introduce relevant concepts and literature necessary for understanding and analysing the phenomenon of hackers’ political involvement in international conflicts. In the second section, I present the case study of KillNet’s evolution, main characteristics, and actions. In the third part, I analyse and discuss the data collected, pinpointing implications for the future of cyberspace. Lastly, I put forward the conclusions of this research and future possible research topics.

During the research, I encountered some limitations in data collection and analysis. A key limitation was the language barrier, as I am not a Russian speaker but had to analyse content in Russian. To address this, I used machine translation (Google translate) and sought assistance from a native Russian speaker, cross-checking data with industry and media reports to enhance reliability. Data sources included primary data from KillNet's main Telegram<sup>4</sup> channel<sup>5</sup> and secondary data from web sources, media, industry and governmental information. Additionally, I used statistics from the social media channel to support my analysis and extracted the content using the online tool Popster<sup>6</sup>.

Another limitation was the vast amount of data generated by the hacker group, especially given the ongoing developments in the war. Therefore, I primarily observed and analysed KillNet through its main Telegram channel, "WE ARE KILLNET",<sup>7</sup> and only briefly scrutinised other channels. The messages included in this thesis date from the 25<sup>th</sup> of February 2022 to the 30<sup>th</sup> of June 2023, concentrating on the messages from the start of the invasion, the most liked, viewed and commented posts, and posts pinned by the hacker group. In some instances, I reference specific messages using the following reference: *reservs/number of the message*<sup>8</sup>, with 'reservs' coming from the name of the main channel 'KillNet\_reservs'. The list of all referenced messages can be requested.

Constructivist research acknowledges the role of the author's biases in shaping ideas and meanings found during the research process. While I strived for objectivity and neutrality, conducting field research inherently involves a level of reflexivity (Hurd, 2008, p. 45). I aimed to avoid prejudices and opinions regarding the invasion of Ukraine or cybercrime while observing and analysing KillNet. Still, I do not limit reflexivity completely since some experiences I encountered as a researcher and individual shaped my image of the research and the case study. Due to my legal and policy background, a bias that I displayed at the beginning of the research was the constant expectation of destructive capabilities from the group, and sometimes disconsidering activities

---

<sup>4</sup> Telegram is a cloud-based messaging platform focused on security and speed. It is widely used in Russia and other Russian speaker countries

<sup>5</sup> A channel is similar to a social media page but has the aspect of a chat; depending on the settings of the owner, participants can either only view posts or react, comment and even post in the respective chat

<sup>6</sup> Popster is an online tool that can generate social media reports and data sets, available at <https://popsters.com/>

<sup>7</sup> NB: up to the end of May 2023, there are more than ten interconnected telegram channels. The main channel can be publicly accessed at the following link: [https://t.me/KillNet\\_reservs](https://t.me/KillNet_reservs).

<sup>8</sup> NB: due to practical considerations, messages are only sometimes references.

without obvious policy-relevant actions were absent. Moreover, from a cultural perspective, as a Romanian, I often found myself at the border between the Western and the Russian understanding of hacktivism.

## **2. Hackers, hacktivism and geopolitics: the process of shaping the cyberspace**

This chapter serves as a foundational framework, introducing crucial concepts and relevant literature essential for comprehending and analysing the phenomenon of hackers' political engagement in international conflicts. Additionally, it explores the construction of cyberspace within the context of international relations and the phenomenon of hacktivism in general terms. The initial section consists of a conceptual note on hacktivism and non-state actors involved in cyber conflict, concepts which form the core focus of this study. Subsequently, the impact of digitalisation on politics and the emergence of military activities in cyberspace, initiated by state and non-state actors, are examined. Moving forward, the chapter introduces the theoretical frameworks constructivism and actor-network theory in relation to hacktivism. Finally, it delves deeper into the phenomenon of political hacking and the intersubjective reality of hacking.

The literature review encompasses a broad array of topics, including but not limited to cyber conflict, cyberpolitics, hacking, hacktivism, and cybercrime. Together, these elements provide a solid foundation for a comprehensive analysis of hackers' political involvement on the international stage.

### **2.1. Conceptual note: Clarifying the definition of Hacktivism**

The existing body of literature on political hacking exhibits conceptual divergence regarding the terminology employed to define it. The term “hacktivism”, coined in 1996 (Illig, 2015), generally refers to acts of protest by the utilisation of electronic means to pursue social and political objectives (Bussolati, 2015, p. 106-109; Hampson, n.d.; Svyrydenko & Mozgin, 2022); the word hacktivism is formed out of the word ‘hack’ and ‘activism’. Some authors use “hacktivism” only to encompass non-violent forms of political hacking (Svyrydenko & Mozgin, 2022), while violent and destructive forms are classified as cyberterrorism (Denning, 2001; Svyrydenko & Mozgin, 2022). However, the precise definition of violence in cyberspace remains undetermined, generally referring to the destructive offensive. Additionally, patriotic hacking is considered a subclassification of hacktivism and is pursued for nationalistic motives (Bussolati, 2015, p. 111; Maurer, 2018, pp. 146–149). In short, hacktivism can be understood as ‘hacking with a cause’.



In academic literature, the key distinction between hacktivism and cybercrime lies in the purpose behind the hacking activities. While cybercrime is carried out for economic gain, hacktivism aims to convey a social or political message (Hampson, 2012; Ireland, 2022; Knapp, 2015)<sup>9</sup>. Nevertheless, these purposes often intertwine or change over time (Maurer, 2018, p. 152). Financial motivations are pursued through the establishment of cybercrime organisations which provide hack-for-hire services or act as cyber proxies for states (Bussolati, 2015, p. 109; Dumbrava, 2012; Maurer, 2018). Conversely, political motivations revolved around advocating for internet freedom, information liberalisation, patriotism, and other ideological motives (Denning, 2001; Ireland, 2022; Li, 2013). It is important to note that the legality of activities falling under hacktivism can vary based on legislative systems and definitions of cybercrime (Hampson, 2012; Ireland, 2022; Knapp, 2015). Some actions may be considered criminal, while others are legal forms of freedom of expression (Hampson, 2012). In certain circumstances, some authors even concluded that hacktivism conducted through DDoS attacks could or should be a legal form of protest (Hampson, 2012; Li, 2013; Svyrydenko & Mozgin, 2022).

In this thesis, through the term “hacktivism”, I refer to political hacking indiscriminately of whether they are considered legal or illegal, ‘violent’ or ‘non-violent’, related to a state. I exclude the term cyberterrorism because it creates confusion regarding the difference between violence and non-violence in cyberspace and may also be linked with traditional terrorism, which falls beyond the scope of this thesis. When applicable, specific references will be made to patriotic hacking. Lastly, through the concept of non-state actors, I refer to any actor, whether an individual or a group, that is not a state or formally related to a state; formal relations include service provision or employment. The term “cyber criminals” is not used since the thesis focuses specifically on the phenomenon of political hacking rather than the broader scope of cybercrime. By avoiding essentialising or romanticising hacker groups as either heroes or villains, we can focus on the intricate and context-dependent processes that define their existence and agency.

## **2.2. The construction of cyberspace geopolitics**

The rapid development of the internet and digital technologies since the 1980s has transformed cyberspace into an integral aspect of our modern lives (Powers & Jablonski, 2015). Not only are digital technologies used for communication, but entire parts of our social and political lives are

---

<sup>9</sup> E.g. “Worms Against Nuclear Killers.”

fully embedded in cyberspace (Bussolati, 2015, p. 106). There we interact with our family, friends, and various services, engage in social activism to promote preferred policies and witness political leaders sharing their messages and visions. Moreover, numerous sectors, including public administration, finance, justice, health, and education, have been fully digitalised (Cerf et al., 2014). While these advancements have improved our lives, they have also exposed vulnerabilities that can be exploited for coercive purposes (Guiora, 2017; Luppicini, n.d.; Maurer, 2018). As presented below, the material and social importance of ICTs, led to the recognition of cyberattacks as serious crimes and potential threats to national and international security.

Over time, cyberspace was constructed as a new dimension of international politics (Reardon & Choucri, 2012). Worldwide, states are increasing their cyber capabilities, creating cyber security strategies and entering into international dialogue surrounding cybersecurity. A few months before the Russian invasion of Ukraine, during the US-Russia summit in June 2021 (CBSnews, 2021), cybersecurity emerged as a key topic alongside longstanding concerns like nuclear proliferation and human rights. While the latter two topics have been significant themes in international relations for many years, cybersecurity has gained prominence more recently. President Biden mentioned giving During this summit Vladimir Putin a list of industries that must be off-limits from Russian hackers; otherwise, retaliation can be expected. According to Hoffman (2007), hybrid war is a conflict that combines conventional, irregular, cyber, and information warfare; this type of hybrid war is believed to will be the norm in future conflicts (Atrews, 2020; Bussolati, 2015; Leuprecht et al., 2019). Hence, cyberspace has become a new battleground for pursuing political interests at the international level, leading to new insecurities.

Fortunately, we could see the adoption and promotion of restraint (GCSC, 2019) in direct interstate cyberconflicts. While attacks still exist and are ongoing, the level of these attacks is not reaching the full destructive potential of states' cyber capabilities (Klimburg, 2017; Maurer, 2018; Valeriano & Maness, 2015). This is primarily due to international politics and norms, which, even if not directly coercive, make states think twice before pursuing destructive offensive in the cyber realm. However, the phenomenon observed by many scholars is that cyber conflicts are usually conducted indirectly through non-state actors, which are under different levels of state control (Dwan et al., 2022; Goode, 2015; Jensen, 2017; Klimburg, 2017; Maurer, 2018). This allows states

to invoke plausible deniability and avoid escalation (Valeriano & Maness, 2015) and, in any case, rely on the uncertainty of the attack's source and the attacker's anonymity.

### 2.3. Non-State Actors in Cyberspace

Authors have divergent opinions on the level of NSAs' capabilities. One of the most comprehensive works on cyber NSAs was done by **Maurer Tim**, a cyber policy scholar and specialist, in his book "Cyber Mercenaries: The State, Hackers and Power". Maurer argues that the power of coercion in cyberspace does not belong only to states but also to multiple non-state actors (Maurer, 2018). In his view, the main cybersecurity threats are developed or deployed by what he calls "cyber proxies" and not by the states themselves (Maurer, 2018). This opinion is shared amongst many scholars (Bussolati, 2015; Dwan et al., 2022; Goode, 2015; Hollis, 2021; Jensen, 2017; Klimburg, 2017). On the other side, hacker groups have been described as "weapons of fear" that primarily conduct "toothless" operations (Valeriano & Maness, 2015, p. 187). Further, Ben Buchanan argues that "shaping" is the best way to describe how cyber capabilities have been used by states and their proxies (Berry, 2022) since hackers can shape elections, societies, narratives and policies.

A distinctive feature of cyber proxies, as opposed to traditional mercenaries, is that the former has become the norm, while state force has become the exception (Maurer, 2018; Nye, 2011, p. 123). The privatisation of security, even in ordinary circumstances, is recognised to diminish state power (Abrahamsen & Williams, 2009). While state-funded operations often possess highly destructive capabilities, they are thought to be frequently carried out through proxies. These cyber proxies operate under varying degrees of state control, ranging from quasi-governmental entities to receiving financial assistance or mere approval from the host government (Maurer, 2018). However, hackers do not follow the same normative behaviours that states are used to in international relations; deterrence and restraint theories cannot shape and predict the behaviour of NSAs (Valeriano & Maness, 2015, pp. 187). In this context, the question arises as to whether the concepts of restraint and deterrence can elucidate state behaviour when their actions become obscured and intertwined with those of non-state actors.

Nevertheless, outside of state activity, hacktivists operating globally use hacking for political and social change (Bussolati, 2015, p. 106). Digital technologies' availability and mass adoption created a cyber dimension of international politics beyond the state (Berry, 2022), a dimension in

which hacker collectives interact with states. Moreover, these non-state actors can pursue their political motives without traditional geographical constraints (Paganini, 2022). Unlike conventional ways of conducting politics, information technology allows individuals and groups to connect easily, create collective identities, and spread ideas and narratives globally (Reardon & Choucri, 2012, p. 9). These hacktivists represent important non-state actors in hybrid wars because they may operate as state proxies, allies or adversaries and impact the battle's political, social, and economic facets. Therefore, hacktivists are relevant NSAs in international cyberpolitics.

“Anarchy is what states make of it” (Wendt, 1992) becomes a very relevant phrase when it comes to hacktivists and the use of proxies in cyberspace. Different regimes, such as state agents, unlawful combatants, cybercrime or cyberterrorism, can apply at the same time to political hacking depending on the national legislations or perspectives on digital sovereignty (Bussolati, 2015; Goode, 2015; Hardy, 2010; Jensen, 2017). These ‘virtual’ groups sometimes remain outside legal regulation due to normative or cooperation deficits (Tsagourias, 2016). There is no certainty that if a patriotic hacker or a group of hacktivists launches an attack against another state, the host state will cooperate in punishing the culprit. The reasons can vary from ideational to legal to the fact that those individuals were used as proxies. This normative ambiguity favours the rise of the phenomenon of political hacking.

Cyberattacks' complexity, ambiguity, and multidimensionality blur the lines between war and peace, state and non-state actors, and military and civilian sectors (Bussolati, 2015; Svyrydenko & Mozgin, 2022). With cyber-attacks, different actors can inflict physical, digital, economic, psychological and societal harm beyond traditional boundaries (Atrewns, 2022, Agrafiotis et al., 2018). Moreover, the national and international regimes are unclear regarding what cyberattacks are deemed acceptable or unacceptable and the regime applicable to the individuals behind the hacks (Goode, 2015; Jensen, 2017). The insecurities present in the physical space were transposed into a new domain: cyberspace. However, compared to physical vulnerabilities, the reality of cyberattacks is that anybody, even just a small group of people or individuals, can disturb systems and cause harm remotely globally.

## **2.4. Constructivism and Actor Network Theory for connecting the social and material of political hacking**

Using constructivism can help understand geopolitics in cyberspace beyond the simple material understanding of the technologies that compose it (Branch, 2018). Constructivism is especially important given the ambiguity and multidimensionality of cyberattacks conducted by both state and non-state actors (Bussolati, 2015; Svyrydenko & Mozgin, 2022). By understanding the constructed meanings and implications of hacking within cyberspace, we can gain valuable insights into its role in shaping international relations. Subsequently, understanding motivations and how hackers frame their intersubjective identity will help forecast future behaviour.

The main argument in constructivist theory is that foreign policy is shaped not only by power dynamics but also by ideas, beliefs and cultural identities. Unlike realist focus on power dynamics and pragmatic factors such as material power or economic interests, constructivism argues that actors in international relations are also driven by ‘ideational factors’ (Branch, 2018; Wendt, 1992; Finnemore & Sikkink, 2001, p. 393; Hurd, 2008). Constructivists acknowledge that not only material power dynamics but also ideational factors shape actors' interests; it evokes the importance of ideas, collective meanings, and expectations in creating social constructs (Hurd, 2008; Wall, 2012). The shaping of international politics goes beyond individual beliefs; it encompasses intersubjective ideas shared among people and institutionalised through practices and identities.

Branch (2018) argues that technology needs a ‘hybrid’ understanding and advocates for the importance of the intersection between material and ideational factors. Constructivist authors dominated the literature regarding cyberspace politics, while realism was more prominent in cybersecurity (Reardon & Choucrist, n.d., p. 6). Policy literature is taking realist stances, concerned with power dynamics and responsibility in cyberspace (GCSC, 2019; UNGGE, 2021). In contrast, the academic literature is focused on the role of digital technologies in generating ideas with transformative power (Branch, 2018; Reardon & Choucrist, 2012, p. 22).

Constructivism can help understand actors' involvement in the cyber conflict surrounding the Russian invasion of Ukraine. The Russian invasion of Ukraine has been analysed and explained through constructivist lenses (Götz & Staun, 2022). Götz and Staun (2022) examined the motives behind the invasion through the lenses of strategic culture, explaining how Russian political

leaders and elites share discourses and narratives based on socially constructed interpretations of history, geography and culture. Similarly, socially constructed interpretations of hacktivism may drive Russian patriotic hackers to pursue a pro-invasion discourse. These, in turn, can convince individuals to support hacktivist activities and join them.

Moreover, Branch proposes the combination of constructivism with Actor-Network Theory to link technology's social component with its material aspects (Branch, 2018). ANT serves as an analytical tool for exploring the interactions between human and non-human actors within networks of relationships (Cresswell et al., 2010, Latour, 1987 in Branch 2018, pp. 110). ANT logic challenges the conventional distinction between social and technological factors and argues that both are equally important in shaping social phenomena (Grabher, 2009; Hurd, 2008, p. 46; Jóhannesson & Bærenholdt, 2009). Using ANT logic, hacker groups must be examined in their social-material realities. This allows us to appreciate the complexity of hacker networks and avoid simplistic or deterministic explanations. Moving from small-scale processes to larger macro-level outcomes is achieved by considering the influential impact of ideas that originate and spread through interconnected networks, both limiting and propelling the development of those (Branch, 2018, p. 111). Therefore, combining Constructivism and ANT logic offers a compelling approach to understanding the complex interplay between social and technological factors in shaping the phenomenon of political hacking.

## **2.5. Idea, identity, and collectivity: Intersubjective reality of politically motivated hacking**

The identities and motives of cyberattack hackers are diverse and driven by various factors, including political beliefs, recognition, nationalism, and public attention. Even if NSAs operating in cyberspace can significantly differ in size, internal structure, motivations, and relationship with the state, hacking creates its intersubjective reality.

### **2.5.1. *The culture of hackers***

Hacktivism, and hacking more generally, has its own culture, characteristics and realities (Dremluga, 2014). Hacker culture is defined by small intimate networks but large collegial networks organised through chat rooms, forums and other online communication tools (Holt et al., 2012). Today, alongside these forums, social media platforms are used for internal communication and engaging the wider public. Other characteristics include untraditional organisation and leadership based on decentralisation and interconnectedness of collegial networks (Dumbrava,

2012). These actors can range from small and independent entities to larger transnational groups. Their organisational structure may exhibit informality, lack a clear chain of command, or evolve into complex, formal, and hierarchically structured entities (Dremluga, 2014; Dumbrava, 2012). Remoteness, transnational reach, anonymity and the ease of escaping justice systems (Dremluga, 2014; Dumbrava, 2012) are a few other characteristics that attract individuals to be members of the hacker collectives.

The incentives behind hacker groups getting involved in a cyber conflict are not purely material or altruistic. Maurer argues that previous differentiation between financially motivated and politically motivated actors does not help understand hackers since their motives proved to change or be intertwined (Maurer, 2018, p. 152). While internet freedom, information freedom (Illig, 2015) and nationalism are powerful drivers (Maurer, 2018, p. 146), in the past, there were examples when these motivations were intertwined or replaced by financial reasons (Hampson, n.d., Maurer, 2018, p. 152). Therefore, hacker collectives can be guided by intertwined economic, political, ideological, or social factors.

Even if they have a wide range of motivations ranging from materialistic reasons to recognition and political motives, hacker collectives are, after all, social networks (Holt et al., 2012). Group belonging and recognition by other hackers are also powerful drivers (Dremluga, 2014, p. 160; Holt et al., 2012). The reality is that a limited number of members are highly skilled, and skills lead to centrality in group and peer attention (Holt et al., 2012). Skills bring hackers recognition inside the group, hence successful hackers often feel the need to communicate and share their knowledge and experience. Thus, learning within the hacker world is a combination of individual and collective efforts, with more skilled hackers openly sharing information (Holt et al., 2012).

While capabilities vary between individuals and groups, hacktivism often relies on Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks. Dos/Ddos attacks temporarily affect the availability of an online resource by flooding it with a high volume of accessing requests. These attacks are easy to deploy and require minimal knowledge and resources (Illig, 2015; Svyrydenko & Mozgin, 2022). Other attacks include phishing campaigns, virtual Sit-ins, Site Defacements, Site redirects, and Site parodies. Because the expertise and resources involved are minimal, hackers do them voluntarily or as an exercise. These attacks aim to capture attention within or outside the group. Hacktivists can also use more complex hacks involving data theft,

leaks or destructive malware, but typically these attacks are associated with advanced persistent threats carried out by criminal organisations or state-sponsored groups (CISA, 2022). Hence, hacking activities vary in complexity and purposes, with hacktivism often relying on simple but attention-grabbing tactics.

### **2.5.2. Political hacking**

The role of the internet in political activism has been recognised since 2001 (Denning, 2001), with hacktivist attacks recorded as early as 1989. One of the first notable politically motivated cyberattacks was “the Wank Worm” attack in 1989, which targeted NASA, the US Department of Energy, CERN, and Riken. The attack included the phrase “Worms Against Nuclear Killers” (Denning, 2001, p. 22), driven by political opposition of the hackers to nuclear weapons and demonstrating the intent to interfere in international security and the nuclear weapons regime. Further, in 2008 Russian patriotic hackers conducted large-scale Ddos attacks against Estonian and Georgian private and public sectors (Bussolati, 2015, p. 102). Hacktivism activities have been widely present also in the Middle East conflicts (Ireland, 2022; Itayc, 2022; Valeriano & Maness, 2015).

Today, hacktivism is often associated with the “Anonymous” group, which started as a movement against internet censorship (Knappenberger, 2012). Over time it evolved into a decentralised movement with a wide range of political motivations, such as fighting against authoritarian regimes (Ireland, 2022), freedom of speech, and civil rights (Svyrydenko & Mozgin, 2022). Anonymous even conducted contradictory campaigns, #OpTrump and #OpHillaryClinton, supporting candidates in the 2020 US elections campaigns (CheckPoint, 2022), showing the diversity of political affiliations.

The black box of hacker groups and their involvement on the international stage are far from being understood. Although the main cybersecurity threats are developed or deployed by what Maurer calls “cyber proxies” (Maurer, 2018) and not by the states themselves, the NSAs phenomenon is empirically an underresearched field of Cybersecurity (*Guiora, 2017; Maurer, 2018, p.151*). There has been research on the Anonymous group (Hardy, 2010; Ireland, 2022; Li, n.d.; Svyrydenko & Mozgin, 2022), but largely, the political activism of hacker groups has been left aside. Literature concerning the involvement of NSAs in cyber conflict has mainly focused on the attribution of



their actions to states (Bussolati, 2015; Tsagourias, 2016), the right to self-defence (Bussolati, 2015) or escalatory risk (Maurer, 2018, p. 151).

A stereotypical image of a hacker was that of an “introverted and unshaven Russian male glued to his computer” (Wall, 2012, p. 5), committing crimes for financial reasons. This is how a cybercriminal would be defined. And this is the Western construction of Russian hackers; they are socially constructed as cybercriminals (Wall, 2012). On the other side, hacktivism can have a positive connotation for civil society (Hampson, 2012; Knapp, 2015), often associated with the idea of fighting for a cause (Dremluga, 2014). Anonymous national chapters emerged in multiple countries as a response to political inequalities and injustices, fighting against corruption, authoritarian regimes, ‘capitalist slavery’ and internet censorship (Hardy, 2010; Ireland, 2022; Li, n.d.; Svyrydenko & Mozgin, 2022). Anonymous created a widespread positive perception of its hacktivism, making hacking a way to fight against authoritarian regimes and promote internet freedom. Hence, the hacker is no longer ‘an unshaven Russian man’ but a freedom fighter hidden under the representative mask of an ‘anonymous hero’.

Nevertheless, unlike state actors or traditional non-state groups involved in kinetic warfare, hacktivists typically do not solely pursue military objectives aimed at power outcomes (Bussolati, 2015). An essential element for hacktivists is public attention and opinion (Dremluga, 2014; Ireland, 2022). Even if public support for hacktivism is divergent, certain circumstances make the public support more hacktivism. Such factors include the lack of trust in authorities, utilitarianism of the cause or if pursued as effective civic participation (Ireland, 2022). Dremluga (2014) argues that public support is considerably present in Russia, with civil society perceiving hackers as heroes fighting for Internet Freedom, and even if officially a crime, courts do not recognise hacking as a dangerous crime (Dremluga, 2014, p. 160). Unsurprisingly, hacktivism and other forms of political hacking are often attention-seeking oriented rather than leading to destructive results; hacktivism loses its meaning when the public does not award attention to it.

Therefore, the perspective from which politically motivated non-state actors (NSAs) in cyber conflict are analysed is essential. While states construct hacking as a criminal activity, hackers construct it as a freedom-fighting tool (Ireland, 2022; Knappenberger, 2012). Governments and corporations may perceive hacker collectives involved in cyber operations as criminals, security threats, or cyberterrorism (Svyrydenko & Mozgin, 2022, pp. 42–42). On the other side, the groups

themselves identify as activists or heroes seeking public support and attention. Both governments and hacker collectives try to convince the same actor: the public/civil society. Hence, socially constructed meanings are being given to cyberspace, cyberattacks, and hacking by states (Wendt, 1992) and actors beyond the state.

### **3. The birth of Russian Hacktivism: the case study of KillNet**

In this chapter, I present and analyse collected data regarding KillNet hacker collective. By following the actors within the network on telegram and web sources over the past year, I gained insights into how KillNet navigates and operate in cyber conflict. Following the ANT's logic (Luppici, 2014; Coleman, 2010), I showcase how KillNet interacts with social and material components of cyberspace and frame their intersubjective reality. By looking at micro-level interactions inside the network, I observed how the hacker group mobilised resources, recruited members, communicated messages and influenced public opinion through their activities. Additionally, I examine the challenges and obstacles that hacker group encounters from other actors, including law enforcement agencies, rival groups, or financial difficulties.

I start by providing some background information on the Russian invasion of Ukraine and its cyber dimension. Following, I provide general information regarding the creation and organisation of the group continuing with their tactics and instruments. Finally, I present in detail their communication strategy and discourse.

#### **3.1. Background information**

In order to understand the information regarding the case study of this thesis, KillNet, I will provide some background information related to the narrative pursued behind the Russian Federation's invasion of Ukraine and the cyber dimension of the situation.

On the 24<sup>th</sup> of February 2022, the Russian Federation launched a full-scale invasion of Ukraine, viewing it as a legitimate military operation. In one of his first speeches, the President of the Russian Federation, Vladimir Putin, referred to the authorisation of the 'special military operation in Ukraine' as a legitimate action taken to help the people residing on the territory of Ukraine, justified on the premises of the article 51 part 7<sup>th</sup> of the United Nations Charter (individual and collective self-defence), on the approval of The State Council of the Russian Federation and the Friendship and mutual assistance treaties with the Donetsk People's Republic and Luhansk

People's republic ("Russia-Ukraine Crisis," 2022). Notably, the invasion is deemed as a grave infringement of international law by the Ukrainian people and Western countries, which helped Ukraine to resist Russia (Congressional Research Service, 2023; European Commission, 2022; European Council, 2023). The discursive expressions that Putin pursues are that the operation strives to achieve 'de-militarization' and 'de-Nazification' of Ukraine and help/save the people residing in Ukrainian territory, including Russian citizens ("Russia-Ukraine Crisis," 2022). In short, Putin's discourse emphasises the operation's normative legitimacy and the need to protect the people.

The invasion displayed a hybrid nature, and the cyber dimension impacted and involved not only the belligerent states but also many other state and non-state actors. On the 23<sup>rd</sup> of February 2022, Microsoft observed the cyberweapon 'Foxblade' – a trojan horse wiper – and an entire wave of cyberattacks being deployed against Ukraine (B. Smith, 2022); Microsoft is and was the leading actor in supporting Ukraine in repelling cyberattacks. Hacker groups such as Anonymous, Conti, KillNet, and others started to pick sides (Przetacznik & Tarpova, 2022; Svyrydenko & Mozgin, 2022; Yildirim, 2022). The Ukrainian government openly asked the hacker community to form an IT Army of Ukraine to defend Ukraine and strike Russia (Cluley, 2022). Individuals, companies and state agencies were warned (CISA, 2022; GoogleTAG, 2023; B. Smith, 2022) that they have to improve their cybersecurity strategies. Increased cyberattacks were confirmed, especially in countries near Russia, such as Romania, Lithuania, Estonia and Georgia (Check Point Research Team, 2022).

On the 20th of April 2022, Five Eyes<sup>10</sup> reported three categories of pro-Russia actors performing in cyberspace on the premises of the invasion: state-sponsored, Russia-aligned cyber threat groups and cybercrime groups that pledged their support for Russia (CISA, 2022). State-sponsored cyber actors, also called Advanced Persistent Threat groups (APTs), are up to date the most prominent threat and often with destructive capabilities (CISA, 2022, p. 3); these include The Russian Federal Security Service (FSB), Russian General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center, and GRU's Main Center for Special Technologies. Russia-Aligned cyber threat groups are considered APTs (state-sponsored) but identified by the industry, while states do

---

<sup>10</sup> Five Eyes is an international intelligence cooperation mechanism between the United States, Australia, Canada, New Zealand, and the United Kingdom.

not attribute their actions officially to Russia. Cybercrime groups are “typically financially motivated cyber actors” (CISA, 2022, p. 8) exploiting vulnerabilities or deploying ransomware for economic return, the main difference being that neither states nor industry reports classify them as state-sponsored. The authorities enhance that the former will continue to act on financial premises, and not too much attention is given to their political involvement.

### 3.2. Killnet general overview

*"Before the special military operation, we left the darknet and joined Russia's mission. Everything we have done since the very first day is only for the sake of helping our country [Russia]. Maybe that is the only thing that makes us different. Today we stand for Russia and are heroes for our country, but in other countries, we commit crimes."*<sup>11</sup>

Killmilk – the founder and leader of Killnet

On the 25<sup>th</sup> of February, one day after the official start of the invasion, Killnet publicly expressed its support for Russia’s ‘special operation’. Before the invasion, around October 2022, the leader of Killnet, known under the alias Killmilk, created Killnet as a DDoS Service (reserves/2858). When the invasion of Ukraine started, and Anonymous attacked Russian actors (Svyrydenko & Mozgin, 2022, p. 44), Killmilk allegedly stopped its financial activity and switched the purpose of KillNet it turned into hacktivism (reserves/2858). In order to make its stances available to the public, Killnet has been using the social media platform Telegram to create its channels and groups. The first official mention of Killnet was in the previously mentioned CISA report (2022) being classified as a Russian-aligned cybercrime group.

As a preliminary note, I could not find any official links between the Russian government and Killnet. While the group asserts it does not have any relations with the Russian authorities (reserves/2858), and their activities seem to be more low-key-hacktivist activities rather than state-sponsored attacks (Riggi, 2023), it is also possible that state agents are involved with the knowledge or without the knowledge of the network and its leaders.

---

<sup>11</sup>(Killmilk, Podcast Legitiamte Question, 2022)

Killnet runs a consistent and evolving global campaign in favour of the Russian government (CheckPoint, 2022). Their attacks are pursued under the rhetoric that anyone who is against Russia is against Killnet (reservs/2428,reservs/2520). In their pinned messages is emphasised the need to create a Russian cyber army (reservs/244), a global network backed by the “International hacker alliance” (reservs/304). Since the beginning, they clarified that they fight against the Nazism present in Ukraine (reservs/13) and Western imperialism. They consider that “half of the world is supplying nazis with money, weapons, equipment” (reservs/2868). The hashtags used to individualise their posts also confirm this narrative; the top 20 hashtags include #demilitarisation, #stopnazis, #Russia, #MinistryofDefence, #stopnato and #germanyrip (see annexe .

Another prominent idea pursued since the start of the invasion was the enmity relation towards Anonymous. Their discourse at the beginning of the chat is focused heavily on Anonymous (reservs/4, reservs/5), and their first attacks are against Anonymous's website (reservs/6). Their top 20 hashtags include #anonymous, #stopfakeanonymous and #trueanonymous (See annexe I). Killnet is accusing Anonymous, which declared war on Russia, of being a ‘fake Anonymous’ and being allied with the US government. On the other side, Killnet perceives its actions as ‘real hacktivism’ and enhances this multiple times on its channel, while actions conducted by Anonymous are ‘fake hacktivism’. It can be seen that the group's discourse is heavily focused on the ‘hacktivist identity’ which Anonymous group built in the past.

### **3.3. Organisation**

It is unsure how large the hacker collective is, but it is composed of members from multiple interconnected hacker groups and even novices. The most prominent name is Killmilk, who is the alleged leader and founder of the group. An interesting affirmation is that if KillNet had been constructed after a “Dark format” (reservs/725), the movement would have been way more effective in its attacks. The central management also includes the leader Killmilk, a foreign secretary available at the telegram account @kill\_here, and a headquarters clerk, @killnet\_mirror. On September 29<sup>th</sup> 2022, Killnet reported that 14 hacker groups are parts of Killnet, and thus, “Killnet is no longer a group... is a new global hacker religion in the cyberspace, protecting the interests of the Russian Federation!” (reservs/2900). Killnet asserts that they created hundreds of detachments in CIS countries - former Soviet Union States (resrvs/2858). Names that are affiliated include but are not limited to Anonymous Russia,

Anonymous Sudan, Conti, REvil, Xacknet, NoName057. Xacknet has confirmed past affiliations with the Russian Government, while Conti and REvil are known for their aggressive cyber operations.

In June 2023, the syntagm ‘Darknet Parliament’ was referenced as the deciding body of the collective, announcing a very important attack that ended up only with DDoS attacks against European Investment Bank (EIB):

*“Three Heads of Hacker Groups from Russia and Sudan Held a Regular Meeting in the Darknet Parliament, and came to a Common Decision: × Solution No. 0191 - Today We are Starting to Impose Sanction on the European Banking Transfer Systems Sepa, IBAN, Wire, SWIFT, Wise.!”* (reservs/6948).

On April 4<sup>th</sup>, they launched their own training programme called “Dark School” (reserves/5967)<sup>12</sup>. The intent is to offer courses for “conducting professional cyber war or increasing the balance of your wallet”. These courses include DDOS (L7/4), OSINT/DEANON (Cyber Intelligence), Pegasus (Spyware for Android/IOS), Social Engineering, Methods of cyber warfare (Psychology and action on the subconscious of any participant in the World Wide Web) and others. Learning is available in Russian, English, Spanish and Hindi. The price of the package course is 500\$, and it includes private video lessons, manuals, and personal communication with instructors 24/7 for two weeks. Participants will receive an updated methodology every 30 days for one year. Training is supposed to start only when a group reaches 2000 participants. On the 16<sup>th</sup> of April 2023, they announced that applications for group 2 had started (reservs/6201); hence, supposedly, over 2000 people registered already for the first group. Evidence in this sense also comes from the fact that the third most liked post (66k) is dedicated to the Dark School (reservs/6063). At the end of the training, the participants will receive a certification with the mention “HAVE PASSED SPECIAL CYBER TRAINING IN THE RANKS OF THE PRO-RUSSIAN HACKER GROUP KILLNET”, and particularly active students will be invited into the team.

From the content of their social media and industry reports (Riggi, 2023; Yildirim, 2022), results show that ‘Zarya’ and ‘Black skills’ (reservs/581, reservs/1151) are highly important subteams which conduct the main offensive. In May 2022, Killnet launched a hiring campaign looking for hackers, programmers, Osinters (open-source intelligence gatherers), and virus analysts. A skill

---

<sup>12</sup> Information provided by the group can be accessed at <https://telegra.ph/DARK-SHKOLA---KILLNET-04-04>

that was ‘welcomed’ to all positions was that of ‘social engineering’<sup>13</sup>. If Zarya is composed indeed out of these kinds of members, killnet capabilities might extend way beyond DDoS attacks and have a complete cyber military operational team. Black Skills is supposed to be an organised group with its own rules and goals, consisting of 24 divisions (support department, intelligence unit, public communication department, scientific centre, security service) with complete synchronisation, and 24/7 hotline (reservs/5681, reservs/5691). At the end of March 2023, allegedly, over 3000 applications have been received (reservs/5898). Black Skills is constructed as a private military hacker and is looking for investors (reservs/5895). If these capabilities to conduct intelligence gathering and conduct offensive, even destructive attacks, are truly achieved, Killnet poses a significant threat to governments and individuals.

The group faced significant financial difficulties and has considered multiple restructurations. The group displayed financial difficulties since 2022 (reservs/2858) and desperation in April 2023 due to a lack of funds and external attacks on their servers (reservs/6339). In September 2022, in one forwarded message from KillMilk’s telegram channel, it was explained how people distorted perspectives on hackers as being rich and influential (reservs/2858). Killmilk argues that he desperately asked the Russian Federation and the Russian businessman for help, but not even a single one of them helped. Killnet asserted multiple times that the group did not receive funds from governments (reservs/2858, reservs/2829, reservs/6277). Further, KillMilk emphasises that he spent all his financial resources on the cause and borrowed money for it, and desperately asked for help from the Russian government and the businessman of the Russian Federation. Later in April 2023, Killmilk addressed the group that while Killnet is the “loudest” group (reservs/6339), it is also the poorest. This is supposed to change, their ‘altruism’ being over and acknowledging that they cannot survive on donations. Further, Killmilk had allegedly exited the group for a period to focus rather on the creation of Black skills (Riggi, 2023). While they will stay dedicated to the Russian mission, they will start taking orders from private entities and states (reservs/6339) through their new private military hacker company: Black Skills. Nevertheless, these attacks will only be directed outside Russian territory and the CIS.

---

<sup>13</sup> The full announcement is available at <https://telegra.ph/Nabor-Zarya-05-08>

### 3.4. Tactics and Instruments

Killnet itself was, in the beginning, a botnet<sup>14</sup>; Killmilk stated that he ‘created a network of computers’ which helped in the provision of hack-for-hire services and earned well from it (reserves/2858). He emphasised on the main telegram channel that when the ‘special operation’ started, he closed the Killnet as a DDoS service in order to focus ‘all forces’ for Russia (reserves/2858). In June 2022, the botnet had 4.5 million infected devices (reserves/1866).

Targets included the Ukrainian government, Ukrainian companies, as well as states, international organisations and companies from all over the world. Governmental and non-governmental actors were attacked in the US, Italy, Romania, Estonia, Finland, Poland, Japan, and more. More importantly, hospitals have also been their targets (Riggi, 2023). Further, they supposedly attacked Israel for subjugating Palestinians (reserves/6008). Targets also involved high-profile IOs websites such as NATO, European Parliament, EIB. Research from Check Point suggests that by September 2022, only 10% of the group’s attacks were directed towards actors from Ukraine (CheckPoint, 2022). The same report pictures that the focus of Killnet was the immediate vicinity of the conflict, with the highest number of attacks being recorded in Estonia and Latvia (CheckPoint, 2022). Important private targets include Lockheed Martin (reserves/2214), Starlink satellite network (reserves/3565), Lufthansa (reserves/3764), JP Morgan (reserves/3029). The case of Lockheed Martin is interesting since the group became enraged when the President of Ukraine, Volodimir Zelensky, made its first external visit since the start of the invasion. The visit was in the US, during which President Biden promised to provide Ukraine with the new Patriot defence system (Liptak, 2022), which is manufactured by Lockheed Martin.

The attacks are heavily publicised on their Telegram channels. They make calls on their channels for coordinated attacks and threaten the victims in a ‘dooms day’ discourse (reserves/2428, Forescout Vedere Labs, 2022). An example of a group coordination technique is the use of #Germanyrip was used to identify and verify the participation of hacker groups in a coordinated attack against German actors (reserves/4894). The verification was done by posting in the group chats the respective hashtag. #Germanyrip was the second most used hashtag in Killnet's main telegram channel. They claim responsibility for publishing on their telegram channel when they conducted attacks,

---

<sup>14</sup> A ‘botnet’ is a network of bots, compromised computers or devices controlled by a botnet operator to carry out malicious activities.



providing screenshots or links to the affected resources and how long it took for the attack to be repealed. Attacks are repealed in intervals of a few hours or even days. Nevertheless, industry reports assess that the impact of their attacks is minimal compared to what it is promised, the end purpose is to distract and misdirect the defensive resources of the victims (Drenning-Blalock, 2022; Riggi, 2023).

On the financial side, the group seems to be relying on donations from members and the large public, with no evidence of sponsorship from the Russian Government. The group makes use of cryptocurrencies and regularly invites followers to donate (reservs/31, reservs/67), and thanks to those that donate (reservs\_2042). There are over 13 different payment options. They also provide advertising services for products through their main channel (resrvs/5789), asserting that the customer will have the opening to approx. 40k potential customers on a worldwide market. Further, evidence of monetisation of their cyberattacks comes from conducting cybercrimes (hack for hire). Solaris, a Russian darknet marketplace, supposedly donated 44 000\$ in Bitcoin to Killnet (Akartuna, 2023) and allegedly was a close partner to Killnet (killmilk\_rus/145, KillMilk, the leader of KillNet, 2022); Solaris was allegedly attacked by the Ukrainian hacker Alex Holden in December 2022 (Akartuna, 2023). The donations are very closely linked to attacks against Solaris's competition, the dark web market Kraken. However, there is only circumstantial evidence regarding the connection, since Killnet, before becoming a branded hacktivism group, was a bot-for-hire.

Infinity forum on the Dark Web, which Killnet created to be in contact with other hackers and which they call an 'apolitical forum' (reservs/5754, *KillNet\_Threat-Analysis*, n.d.), is used for coordination and communication. Anonymous Russia, Infinity Hacker By (Belarus), Bear IT Army, Deanon Club, Special Attack and Reconnaissance Division - SARD, and National Hackers of Russia are the hacker organisations who are currently listed as official forum members as of January 2023. However, Infinity's goal is to bring together all significant pro-Russian hacktivist organisations. The rhetoric behind the forum is "peace and money, not war" and that while "the war will end... the Dark web will never" (reservs/5754). As a result, it can be anticipated that more hacking groups will be joining the forum as legitimate members.

### 3.5. Communication and public engagement strategy

The First Killnet Telegram channel was created on the 25<sup>th</sup> of February, one day after the invasion started. They use Telegram in order to publicise themselves and release videos, photos, documents, polls and messages addressed to governments and the public. The first channel was closed by Telegram due to infringement of local regulations (reservs/1731); however, immediately, another channel was created alongside many other channels, which remain active until the present. I could identify over other ten channels and bots<sup>15</sup> that are officially recognised by the group itself and there are many other channels that were created without their consent, an aspect which they emphasise on their main channel<sup>16</sup>.

Their communication strategy is complex, including infographics, videos and images that are becoming more and more complex. They are releasing videos on VK and Telegram with dramatic signature sounds for intro and outros. Killnet has its own distinguishable logo and individualises its messages with the phrase “We are KillNet”, which is often used in combination with “we do not forget, we do not forgive, we are legion” and “glory to Russia” as a signature ending. Nevertheless, these signature word sequences are familiar with sequences used by Anonymous in signing their messages: “We are Anonymous. We are legion. We do not forgive, we do not forget. You shall expect us.”.

---

<sup>15</sup> Compared to other platforms, telegram allows user-developers to build their own ‘bots’ which in simple terms means that users can develop their own applications that run entirely on the Telegram platform. Killnet uses these kind of bots for receiving messages from other users in a centralized way or for responding to people questions regarding their activities. See more at <https://core.telegram.org/bots#How%20Do%20Bots%20Work?>

<sup>16</sup> See killnet\_reservs/42, killnet\_reservs/1751, killnet\_reservs/4043. Killnet specified on their channel that people should be aware of these ‘scams’ and unsubscribe from fake channels, further emphasizing their official channels.

<i>Analysed pages</i>	<b>WE ARE KILLNET (<i>Killnet_reservs</i>)</b>
<i>Followers</i>	101 462
<i>Total posts</i>	4 829
<i>Reactions to posts (total)</i>	7 085 401
<i>Comments</i>	51 007
<i>Total Views</i>	154 110 935
<i>ER Day</i>	14.3542%
<i>ER Post</i>	1.4565%
<i>ER View</i>	455.3874%
<i>Average Likes</i>	1467.26
<i>Average Comments</i>	10.56
<i>Average Views</i>	3 1913.63
<i>Period</i>	26.02.2022-30.06.2023

In June 2023, Killnet’s main telegram channel entitled “WE ARE KILLNET” had over 100k followers, 4829 posts, over 7 million reactions, and over 50k comments. Killnnnet’s main channel has an ER per day of 14%, meaning that 14% of its followers interact with the channel on a daily basis and an ER Post. This means that approximately 14 000 people interact (like, share, comment) on a daily basis with the content Killnet is posting. Its ER View is 455% meaning that the number of engagement with the content is more than four times its number of followers; with these SM statistics, the marketing industry would classify Killnet as a mid-tier influencer<sup>18</sup>.

The audience of Killnet is not limited to Russians. The post<sup>19</sup> with the most reactions/likes is made on the 12<sup>th</sup> of September of 2022, and it is a poll in which Killnet asks the audience from what

<sup>17</sup> These statistics are subject to change according to the evolution of the telegram channel. The analysis is based on data substracted on 09/07/2023

<sup>18</sup> Nano influencers = 1,000 and 10,000 followers; Micro influencers = 10,000 and 50,000 followers; Mid-tier influencers = 50,000 and 500,000 followers; Macro influencers = 500,000 and 1,000,000 followers; Celeb/Mega over 1,000,000 followers; see *The Benefits, Pitfalls, and Differences of Influencer Marketing Tiers from Micro to Celeb*, n.d.

<sup>19</sup> Reservs/4278

countries they are and to do so react with the specific emoji (reservs/4278). The post has 146 652 reactions and 257 336 views. Most of the answers were Russians (~144k), followed by Belarusians, Kazakh, Armenian, and one thousand ‘other nationals’<sup>20</sup>. The intent behind the post was apparently to see how multinational the movement is. Moreover, with time, Killnet started making videos in English or provide subtitles (reservs/244). Moreover, when conducting an attack against a certain country, subtitles and audio in the language of that country were provided. Now, some messages posted on their channel include a Russian version followed by an English translation. Killnet puts people to doubt about their countries and accuses European politics being puppeted by America (reservs/25).

One of their tactics is the use of defamatory language and hate speech towards Western societies and the Ukrainian government. Defamatory language and information/‘news’ are addressed and not limited to Ukrainian, European and American officials and NATO countries. President Zelensky and President Biden are often mentioned in their discourse. Unsurprisingly, multiple times LGBTQ connotations are used as defamatory elements towards these actors (reservs/6060). This form of defamatory is especially relevant since Russia is known for its anti-LGBTQ laws, which were expanded in December 2022 (Chernova, 2022). Two of the Hashtags that have the highest engagement rate<sup>21</sup> with users are references to male sexual parts (#уї and #ї). Hence, hate speech is a seemingly useful tactic in their discourse.

Moreover, the communication on the channel and chats seem to be managed in a democratic and inclusive way. The possibility was awarded to participants in the channel to comment on the post, a facility not available since the beginning. It was emphasised that the purpose of chats and comments is to create dialogue, eliminate differences, create peaceful interactions and discussing the events (reservs/1640), with chat rules focused on respect. Polls are used to democratically manage the group chat (reservs/2627). Further, prizes are offered for sharing posts of the main telegram channel (reservs/199). Killnet's most viewed post was a poll on whether to attack or not NATO, with total views reaching almost one million; Killnet was asking the network to help them

<sup>20</sup> NB. some votes were not actually representing a country and did not have a substantial meaning.

<sup>21</sup> Engagement rate = percent of followers that interacted with the content; The term "engagement rate" in social media refers to a statistic that assesses how actively people engage with the content or an account. This indicator is used by individuals, businesses, and organizations to evaluate the success and impact of their social media content and presence

‘make the right choice’. “The destruction of NATO on the network” had an affirmative vote of 99% out of over 180.000 of those who voted.

### 3.6. Collective Identity

Killnet perceives itself more than a group but as an idea and a brand (reservs/4035). Protecting their unique hacktivist identity has been highly important since the beginning (reservs/42, reservs/215). They are also keeping an eye on how the media and industry report on them (reservs/4429(Riggi, 2023)). An interesting development was in June 2023, when the group released a teaser for a future documentary with the theme “24<sup>th</sup> of February the birth of Russian hacktivism”, hence, considering themselves the beginning of Russian Hacktivism.

The group is building a collective identity and community revolving around the hero-like image of Killnet. Multiple discursive expressions are referenced to brotherhood and tries to build a collective meaning: “Fraternal people of Moldova” (reservs 2428), “brothers and sisters”, “killnet stands 24/7 to protect its people”, “comrades”(reservs/2184), “your help” (3764), “you, friends”(reservs/227). Right at the beginning of their Telegram channel, the emphasis was that KILLNET does not support fratricide and the war itself, saying that Russia and Ukraine are one country, accusing Ukraine of being under the rule of businessmen and the West (reservs/10). Further, they use other integrative statements such as “Good morning Russia”, “how are you doing” and they refer to the community as “citizens” (reservs/2466), “my beloved country Ru” (reservs/3137), “cyber mafia”(reservs/2870).

Evidence of the importance given to their identity also comes from various copycats that appeared on telegram. KILLNET monitored and constantly updated the list of those chats/channels that are not part of the movement (reservs/212), prompting followers to unfollow these accounts. These accounts pretended to be Killnet or associates of the latter. Vederes lab found out that some of these groups either tried to commit scams by offering fake DDoS services or just to enjoy the attention offered by the brand KILLNET created (Vederes, p.12). This shows not only the importance KillNet gives to its identity but also the fact that ‘KillNET’ is considered a worthy brand to copy or venerate.

In order to build a positive feeling inside the group chat and the community, the discourse and activities also make use of public sensitive policy topics such as praising the heroism of the soldiers lost in duty (reservs/3840), fighting against drugs (reservs/3764) and paedophiles (reservs/4114).

The Wagner group was described as brilliant, dedicated heroes (reservs/5231). Moreover, Killnet conducts a war on drugs (reservs/3764), with many attacks being directed against illegal marketplaces on the dark web. People were invited to report drug marketplaces and crimes in order for the group to conduct attacks against those (reservs/3764). Further, they make appeal to the public for donations for charitable causes; during the 2022 Christmas period, they gathered donations and bought cell phones for children in boarding schools in Donetsk (reservs/3856), posting ulterior a picture of the bags with phones and a video of the children receiving the gifts (4489). Similarly, they gathered donations for children in orphanages in Russia for New Year's (reservs/4207); Approximately 20.000 euros were gathered and 100 phones and earphones were bought (reservs/4253). In this context, an interesting normative behaviour is displayed through the emphasis that these gifts are exempted from taxation according to the Russian Tax Code. This perception of normative legitimacy has also been displayed by Killmilk, who stated that he is abiding by the law, but when it comes to cybercrimes (KillMilk, 2022). This collective identity based on effective civic participation increases the chances of KillNet being perceived from a positive angle (Ireland, 2022).

*“Our family - our subscribers from Telegram - are a strong support for us, for which we thank them.” – (Interview Killmilk, 2022)*

Evidence of public support for KillNet’s cause comes in many forms ranging from donations to the creation of Killnet Branded items. The idea of the existence of a brand worth venerating was encompassed by Kazhe Oboyma, a Russian singer and one of the donors and supporters of Killnet, in his song “KillnetLow”, created as a form of support for the group. The artist risked and was eventually fired by its music record company (D. Smith, 2023). The song is about Killnet’s heroic activity and tactics and can be listened to on multiple platforms such as YouTube, Spotify, Apple Music or Deezer. Moreover, the jewellery manufacturer HooliganZ launched a series of Jewelry branded with the KILLNET Logo, with allegedly half of the money going to Killnet. HooliganZ posted on their VK<sup>22</sup> social media account that they support Killnet. Evidence that their community supports Russian heroism can be seen through the fact that the second most liked message, which is sending the simple message “Glory to Russia”, has almost 80k likes and 108k views

---

<sup>22</sup> Post available at [https://vk.com/hlgnzzz?w=wall-120167132\\_1953](https://vk.com/hlgnzzz?w=wall-120167132_1953)

(reservs/6671). These connections and relationships within Killnet collective highlight its intricate and complex structure.

## 4. Understanding the future role of Hactivism

*“Hackers are free people, just like artists who wake up in the morning in a good mood and start painting. Likewise, hackers ...read the news about international affairs. If they are patriotic, they begin to make what they see as a fair contribution against those who speak ill of Russia”<sup>23</sup>,*

– Vladimir Putin 2017 (RFE/RL, 2017)

In this chapter, I pinpoint the main findings and implications derived from Killnet’s case study for understanding hacktivism in cyberconflict. The main idea portrayed in this chapter is that meanings and ideational factors inside the hacker collectives have been and will be shaping narratives, policies and geopolitics in cyberspace. The first part covers the intersubjective reality of the Killnet hacker group, explaining how Killnet’s identity is shaped by its socio-technical network. The following section is dedicated to understanding how Killnet’s evolution can be perceived as a switch in hacktivism. The chapter ends with showcasing how publicity plays an important element in the evolution of Killnet and their discourse is as important as their capabilities.

### 4.1. The hacker and the bot: Killnet’s socio-technical network is shaping their identity and discourse

Understanding the dynamics of hacker groups in cyberwar and international relations necessitates the application of constructivist lenses (Branch, 2018; Wendt, 1992; Finnemore & Sikkink, 2001; Hurd, 2008). The Russian-aligned hacker collective Killnet embodies a unique intersubjective reality and set of beliefs that significantly influence their activities. This thesis found that the social construction of national identity, hacker identity and the importance of cyberattacks hacker groups led to the creation and evolution of Killnet. Killnet confirmed that hacker groups have their own intersubjective reality and set of beliefs that glue them together and foster their activities (Dremluga, 2014; Hampson, 2012; Illig, 2015; Maurer, 2018, p. 146). These intersubjective

---

<sup>23</sup> <https://lenta.ru/news/2017/06/01/hudohakeri/>

meanings come from the group's definition and interpretation of themselves as well as from social practices in which they are embedded and which they constitute.

Killnet's formation and evolution can be traced back to the intersection of Russian nationalism (CheckPoint, 2022), hacker culture (Dremluga, 2014), and the significance they attribute to the non-human, commonly referred to as 'the network.' This collective has undergone a process of identity and community building based on ideas and narratives that align with the actions of the Russian state. The rhetoric propagated by Russian leadership ("Russia-Ukraine Crisis," 2022), especially regarding the denazification and protection of Russian speakers during the conflict with Ukraine, is absorbed by the hacker group and reflected in their discourse to their followers. As a result, Killnet has constructed a deeply rooted identity founded on Russian nationalism, which in turn informs their cyberwarfare strategies.

One critical aspect of Killnet's identity formation and cyberwarfare strategies is the transference of traditional political ideas and identities into the virtual realm, commonly referred to as hacktivism. Killnet views itself as a legitimate political actor, making decisions through a 'Dark Parliament,' thereby blurring the lines between traditional state affairs and cyberspace activities. Killnet portrays their actions as acts of heroism and patriotic fighting. They firmly believe that conducting cyberattacks can deter assistance towards Ukraine and inflict harm upon societies opposing Russia, even if no human casualties result from their cyberattacks. Consequently, this construction of cyberattacks can instigate social anxiety (Valeriano & Maness, 2015) among potential targets of cyberattacks, leading to ineffective mobilisation of public resources.

Inside KillNet, the hacker identity is as important as the national identity. To understand Killnet's involvement in cyberattacks against Ukraine and its allies, a comprehensive examination of their intersubjective reality and motivations is essential. While Russian nationalism and political alignment with the Russian Government contribute to their actions, hacktivism's intersubjective reality must be considered as a complementary element. The transformed phrase "We are Anonymous" into "We are KillNet" and their comprehensive discourse regarding 'fake' anonymous reflects that KillNet constructed their identity on concepts of hacktivism pre-defined by Anonymous. Moreover, the identity created by Killnet heavily relies on the 'dark web' identity present in hacker collectives (Dremluga, 2014; Dumbrava, 2012; Holt et al., 2012). Darknet,



“Dark format”, “Dark Parliament” are a few examples of linguistic expressions used by the group to refer to the mysterious anonymous world of hackers.

The network, comprising both human and non-human actants (Branch, 2018; Cresswell et al., 2010), plays a pivotal role in Killnet’s activities. Killnet established a one-sided amity relationship with the Russian Federation and Russian Business men, although there is no evidence support from those, but on the contrary complete ignorance, as the group asserts. The foundation of this relationship is primarily rooted in political alignment with the ‘special military operation’ objectives. Conversely, enmity relations emerge from hate speech and cyberattacks directed at Ukraine and its allies, as well as Anonymous and drug markets. Moreover, Killnet’s reliance on external support and public engagement underscores the significance of the community in shaping the group’s formation and evolution. At the same time, the non-human, the idea of the “network” and the “bot” are important elements of their activities. The bot is more than an instrument but an actant in itself (Latour, 2007). The botnet, named KillNet, which Killmilk was using previous to the invasion in conducting attacks for his personal financial motives, “turned into hacktivism” (reserves/2858). Now KillNet is no longer just a network of computers but a network of hacker groups and individuals. Killnet’s activism is conducted “on the network” (reserves/1731) and a technological-religious reference is made in reserves/4892: “(may) the speed of the network bandwidth be with us”. These human and non-human relations are shaping Killnet’s identity, discourse and beliefs.

#### **4.2. Killnet changed the way hacktivism is to be understood**

Killnet’s transformation has profoundly impacted the way hacktivism will be perceived in the future. In just one year and a half, Killnet transformed from a financial instrument to a group chat on telegram conducting DDoS attacks into an “idea” and prospective private military hacker company. Hence, there were awarded new meanings and purposes to the non-human instrument “Killnet” which was created for financial purposes. Killnet institutionalised the idea of patriotic hacking (Bussolati, 2015; Maurer, 2018, p. 146), giving it can have a life beyond the state. The collective is developing its activities through the recruitment of experienced hackers and criminal networks. Although the idea of Killnet becoming a private cyber mercenary company is yet to have produced significant outcomes, there is evidence of the strong intent of surpassing the current capabilities, especially from discourse and strategic discloses surrounding the Zarya team and

Black. Now, the concern should be that Killnet will eventually display destructive capabilities in the form of encryption—based malware, extortion and wiper malware.

Killnet redefined hacktivism from a disorganised collective effort (Dremluga, 2014; Dumbrava, 2012) into a centralised organisation. Compared to Anonymous, where people could join regardless of political affiliation and operations conducted might even have contradictory political intentions (CheckPoint, 2022), Killnet presents a more organised structure, a clear and consistent political ideology, centralised leadership, a well-established recruitment procedure and a set of tools available for members. It has management, an organigram, a school, functional teams, recruitment procedures, financial strategies, public relations strategy and so on. Moreover, Killnet displays the capacity to organise cooperation between several groups of hackers and direct attacks against the same targets. It is no longer about dispersed small and close circles (Holt et al., 2012) but big organised social collectives.

Killnet highlights in its discourse the importance of financing, especially state sponsorship, complaining about the lack of support from the Russian Government and the Russian businessman. Even so, the political motivation survives and this lack of support and finance from the state is not deterring Killnet from stopping its activities but pushing to develop its own financial capabilities through monetisation of Killnet. While still in its early stages, this strategic move signifies the group's desire for state sponsorship (Maurer, 2018) and recognition, indicating a shift from disorganised hacktivism to a more centralised and purpose-driven organisation. Maurer's idea that the motivations of hacker groups are intertwined, encompassing financial and political motivations, is partially confirmed (Maurer, 2018, p. 146-149). However, even so, the political stance feels more powerful in Killnet's case.

#### **4.3. Killnet is an idea and a brand: why attention matters**

The high and consistent number of followers, likes and comments shows that Killnet enjoys public support in Russia. Either if we consider Killnet as having a good PR strategy or the Russian population drawn towards perceiving hackers in a positive light ((Dremluga, 2014), Killnet successfully engages with the Russian speaker community, portraying themselves as heroes and shifts narratives in favour of Russian. Further, the image of conducting a war on drugs and collective donations for children can make the public support them (Ireland, 2022). Branding

KillNet around heroism and legitimate social causes is intended to increase the acceptability and legitimacy of their actions in the eyes of the public and increase their audience.

In this context, the hybrid social-material understanding of technology (Branch, 2018) is important. Cyberconflict compasses not only traditional material destruction but also a more subtle dimension in the form of social engineering and information warfare. Killnet might not have been a very aggressive NSA, but it is truly an ‘influencer’ of the Russian hacker world. Imagine that tomorrow there will be free general elections in Russia, what is the capability of Killnet to convince people to vote for a candidate of their choice? Similarly, how many people did Killnet succeed in convincing to support the Russian Government in its current military endeavour? Evidence that their community supports the Russian narrative can be seen clearly from the second most liked post, which is sending the simple stating message “Glory to Russia” and asking to see who supports the statement (reservs/6671).

Killnet knows and believes that public relations and media coverage are as important as developing their capabilities. Killnet emphasised that by reading news about the attacks Anonymous conducted, people offer the movement strength and hence offer an “unnatural power” to Anonymous in the network (reservs/5). Moreover, Killnet has recycled the Anonymous hacktivism brand and real geopolitical situations by integrating Anonymous Russia and Anonymous Sudan into the hacker collective. Anonymous Sudan appeared as a pro-Russia actor at the same time when the conflict in Sudan was breaking news worldwide in 2023. While the evidence is inconclusive regarding who is behind these Anonymous groups, they use the previously branded Anonymous idea (Knappenberger, 2012) and other sensitive geopolitical situations (e.g. Israel) to attract attention and the public.

While it is true that state-sponsored operations are more complex and have a destructive purpose, the power of non-state-sponsored operations can also have a relevant impact. Conducting attention-seeking attacks and spreading discourses through social channels in favour of one of the belligerent countries can increase the odds of gaining public support for that state. With Nye’s definition of cyber power as the ability to produce preferred outcomes within cyberspace or outside it through the use of cyber tools (Nye, 2011, p. 123), we can conclude that relevant outcomes in cyberspace can include coercion but also attracting public support for a cause/state and shaping narratives that will further influence policies. In the case of Russia, hackers inside Killnet nurturing

nationalistic sentiments prolong the support for the Russian Government and hence prevent social change from happening. At the same time, they are fully open to being recruited by the Government in order to conduct operations on its behalf as a proxy.

Whether funded or not by the state, the reality is that NSAs construct their own world in which states are welcomed and do enter. Killnet might or might not be a full NSA. Maybe under the mask of anonymity, there are governmental employees, but at the same time, many of the participants and followers of Killnet are not. The important aspect is that Killnet is shaping a narrative towards the support of the actions of the Russian Government and is building a collective identity inside the group based on hacking, Russian nationalism and hatred towards Ukraine and Western societies.

#### **4.4. The future of the hacker and the state**

What we can see in the 2022 invasion of Ukraine is that different NASs pursue different rhetorics on global order, peace and security. Killnet's case is just one representative case on the Russian side. The invasion of Ukraine created a significant shift in the Eastern European cybercrime world (GoogleTAG, 2023) and there are over one hundred groups just in this conflict that are pursuing discourses on the conflict, conducting attacks and mobilising people to get involved in cyber conflict (Yildirim, 2022). While Anonymous and Ukraine's Cyberarmy claim the side of the liberal order and independence of Ukraine, hacker collectives such as Killnet and Conti support ideologically the rhetoric pursued by Russia in occupying Ukraine. Western intelligence agencies assess hacker groups aligned with Russia as threat groups (CISA, 2022), while threat groups and their followers define it as heroism.

The accessibility and wide availability of internet resources are making hacktivism a cheap and easy way to pursue political ideologies. As many authors emphasised, these actors will not cease to be involved in interstate relations (Bussolati, 2015; Ireland, 2022; Maurer, 2018; Tsagourias, 2016). The involvement of these actors combined with the hybrid nature of the future interstate conflict (Atrewns, 2020; Bussolati, 2015; Leuprecht et al., 2019) is complicating relations between states, blurring the difference between state and non-state. However, we could see that both in the case of hackers on the Western side and the Russian side, states are turning a blind eye and ignoring their presence in the conflict. While states can do little to limit the creation of groups like Killnet, they can discourage the phenomenon.

Vladimir Putin's statement on hacktivism showcases the acceptance of hacktivism in international affairs, pointing out the latter as an inspiration for patriotic hackers (RFE/RL, 2017). What is striking in his comment is not only that he somehow shows compassion towards hackers, describing them as "artists", but he states (and believes) that these actors 'contribute' to their country. Nevertheless, in the continuation of the quote, Putin emphasises that his deep belief is that hackers are not able to crucially influence elections and that the Russian Government is not supporting and is not planning to support hackers (RFE/RL, 2017). My argument is that such comments should be avoided and, on the contrary, states should publicly discourage such behaviours on behalf of states.

Policymakers have to be aware of legitimate perceptions of hacktivism (Dremluga, 2014, p. 160; Maurer, 2018, p. 148) when drafting global policies concerning NSAs' involvement in interstate relations. NSAs will need to get involved or be used by states for their benefit. It is unlikely that Russia and Ukraine will view legitimate strict condemnations of hacktivism conducted in their favour. While President Putin argued in 2017 that Russia does not support hackers, in the context of the invasion of Ukraine, there has been no direct discouragement from the Russian Government at the address of hackers. The reciprocal is valid, Western states did not exhibit any discouragement towards Anonymous attacking Russia, while President Zelensky even called on hackers and the IT community to help defend Ukraine (Cluley, 2022)

While it is virtually impossible to limit the creation of groups like Killnet due to the accessibility and wide availability of internet resources, states can manage the phenomenon by subtracting any form of governmental legitimacy (Maurer, 2018, pp. 146–149). Governments should expressly discourage these behaviours by stating that they do not support political hacking on their behalf. Instead of letting hacker groups dictate state behaviour and policy, governments should aim at developing the ability to shape their relationship with these actors. Future policy research could focus on how to balance the structural and ideological factors in the limitation of the phenomenon of politically motivated hacking.

## 5. Conclusions

The main finding of this study is that Killnet, a politically motivated non-state actor, constructs its identity and disseminates narratives in favour of the Russian Government. The group's political involvement is driven by a combination of Russian nationalism, intersubjective meanings attributed to hacktivism, and the social and technical characteristics of cyberspace. Applying constructivism to hackers reveals that they are social actors influenced by the norms and discourses of their communities and the wider international society. Inside Killnet, hacktivists identify themselves as heroes, warriors, and proxies (Maurer, 2018), pursuing diverse interests, from supporting Russia to fighting drug trafficking and creating a community. The emergence of hacktivism as a significant phenomenon in international politics and the interactions within hacker collectives underscore the importance of understanding the interplay between state, non-state actors, human and non-human actants in shaping cyber activities and narratives.

Killnet's evolution showcases how hacker groups have become a new component of international politics through the fusion of Russian nationalism, hacker culture, and the concept of "the network," cyberspace, significantly influencing their identity and discourse. Through looking into their discourse and activities, the study highlights the complexity of hacker networks. The social circles surrounding Killnet display a multifaceted dynamic, encompassing financial contributions, active engagement in illegal activities and military operations and passive support through social media reactions, art, and entertainment. It becomes evident that examining hacker groups in their social-material realities through the use of methods such as Actor-Network Theory and Constructivism allows for a more comprehensive understanding of their complex networks and motivations. In short, the combination of Russian nationalism, hacker culture, and the concept of "the network" has played a pivotal role in forming Killnet's identity and discourse.

The complex public relations strategy employed by Killnet, aimed at gaining public attention and media coverage, underscores the importance of perception and legitimacy in the cyber domain. Killnet's effective public relations campaigns demonstrate their capability to publicise and promote their achievements, utilising the internet as a platform for sharing information and communication at a global level. The use of social media platforms as a means of mobilising civil society and attracting new hacktivist members showcases the role of online engagement in contemporary world. By bringing hacker groups together and the wider public Killnet created a networked civil

democracy inside cyberspace. Therefore future research can look in more detail at how the actions of this group of hacktivists are perceived by international opinion and to what extent they are consistent with generally accepted norms of the rule of law. Further research is needed to assess the real influence these groups have on public opinion and policy decisions, as their impact might be more subtle than initially perceived.

Hacktivism is no longer a bunch of people who conduct low-level DDoS attacks or website defacement (Illig, 2015; Svyrydenko & Mozgin, 2022). Now, hacktivism can be expected to be structured, organised, and effective. Killnet proved that hacker groups can conduct disruptive and orchestrated large-scale DDOS operations in an inter-state conflict while maintaining extensive public relations. Killnet's efforts to surpass the obstacle of not being state-sponsored through the creation of a cybercrime group (company) and eventual state proxy reveal the group's complex strategic approach to garnering financial and political support. Killnet's efforts to overcome the lack of state sponsorship involve the creation of a cybercrime group and an eventual state proxy, signalling the group's strategic approach to gaining financial and political support.

Although Killnet has not fully demonstrated extensive destructive capabilities, it has successfully built a collective and a community, hence, shaping narratives on the war. Hacktivism in cyberspace challenges conventional boundaries and norms of international relations, with Killnet showcasing its ability to shape and disseminate ideas and narratives, indirectly influencing the conflict between Russia and Ukraine. Governmental authorities should take this development seriously to discourage the political involvement of hackers in inter-state affairs.

In one sentence, the case study highlights the significance of nationalism and hacker culture in hacker groups' involvement in international conflicts, wherein intersubjective meanings attributed to hacktivism play a central role in framing their activities.

\*The messages referenced can be publicly accessed on KillNets main telegram channel, killnet\_reservs, or by adding the number to [https://t.me/killnet\\_reservs/](https://t.me/killnet_reservs/) (eg. [https://t.me/killnet\\_reservs/4](https://t.me/killnet_reservs/4)). Upon request I can provide full and partial table of messages.

**Word count:** 13400

## 6. Bibliography

- Abrahamsen, R., & Williams, M. C. (2009). Security Beyond the State: Global Security Assemblages in International Politics. *International Political Sociology*, 3(1), 1–17.  
<https://doi.org/10.1111/j.1749-5687.2008.00060.x>
- Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1). <https://doi.org/10.1093/cybsec/tyy006>
- Akartuna, A. (2023). *Friday the 13th on the Dark Web: \$150 Million Russian Drug Market Solaris Hacked by Rival Market Kraken*. <https://hub.elliptic.co/analysis/friday-the-13th-on-the-dark-web-150-million-russian-drug-market-solaris-hacked-by-rival-market-kraken/>
- Atrews, R. (2020). *Cyberwarfare: Threats, Security, Attacks, and Impact*. *Journal of Information Warfare*, 19(4), 17–28. <https://www.jstor.org/stable/27033642>
- Berry, G. (2022). The hacker and the state: Cyber attacks and the new normal of geopolitics. *Journal of Cyber Policy*, 7(1), Pages 95-96. <https://doi.org/10.1080/23738871.2022.2059385>
- Branch, J. (2018). Technology and Constructivism: Interrogating the Material-Ideational Divide. In *Constructivism Reconsidered: Past, Present and Future*, ed. Ed. By Patrick James, Jarrod Hayes, and Mariano Bertucci (pp. 103–115). University of Michigan Press.
- Bussolati, N. (2015). The Rise of Non-State Actors in Cyberwarfare. In J. D. Ohlin, K. Govern, & C. Finkelstein (Eds.), *Cyber War* (pp. 102–126). Oxford University Press.  
<https://doi.org/10.1093/acprof:oso/9780198717492.003.0007>
- CBSnews (Director). (2021). *Biden and Putin discuss cybersecurity and human rights at Geneva summit*. <https://www.cbsnews.com/video/biden-putin-summit-today-cybersecurity-human-rights-recap-analysis/>



- Cerf, V., Ryan, P., & Senges, M. (2014). Internet Governance Is Our Shared Responsibility. *Journal of Law and Policy for the Information Society*, 10(1).
- Check Point Research Team. (2022). *Resurgence of Increased Cyber Attacks on both Russia and Ukraine, a month into the war* [Industry report]. <https://blog.checkpoint.com/security/resurgence-of-increased-cyber-attacks-on-both-russia-and-ukraine-a-month-into-the-war/>
- CheckPoint. (2022). *The New Era of Hacktivism – State-Mobilized Hacktivism Proliferates to the West and Beyond* [Industry report]. Check Point. <https://research.checkpoint.com/2022/the-new-era-of-hacktivism/>
- Chernova, I. K., Anna. (2022, December 5). *Putin signs expanded anti-LGBTQ laws in Russia, in latest crackdown on rights*. CNN. <https://www.cnn.com/2022/12/05/europe/russia-lgbtq-propaganda-law-signed-by-putin-intl/index.html>
- CISA. (2022). *Five Eyes alert: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure*. Cybersecurity&Infrastructure Security Agency. <https://www.cisa.gov/news-events/alerts/2022/04/20/russian-state-sponsored-and-criminal-cyber-threats-critical>
- Cluley, G. (2022, February 25). *Ukraine calls for volunteer hackers to protect its critical infrastructure and spy on Russian forces* [IT Company]. <https://www.bitdefender.com/blog/hotforsecurity/ukraine-calls-for-volunteer-hackers-to-protect-its-critical-infrastructure-and-spy-on-russian-forces/>
- Congressional Research Service. (2023). *Russia's War Against Ukraine: European Union Responses and U.S.-EU Relations*.
- Cresswell, K. M., Worth, A., & Sheikh, A. (2010). Actor-Network Theory and its role in understanding the implementation of information technology developments in healthcare. *BMC Medical Informatics and Decision Making*, 10(1), Article 1. <https://doi.org/10.1186/1472-6947-10-67>
- Denning, D. E. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. *Naval Postgraduate School*, 1–50.

<https://www.bing.com/ck/a?!&&p=71d1eef0b97b49d6JmltdHM9MTY5MDc2MTYwMCZpZ3VpZD0yYjg3YmExZS03MjdkLTYxMzAtMzQzOC1hOTVhNzNiZDYwMzEmaW5zaWQ9NTlwMA&ptn=3&hsh=3&fclid=2b87ba1e-727d-6130-3438-a95a73bd6031&psq=Activism%2c+Hacktivism%2c+and+Cyberterrorism%3a+The+Internet+as+a+Tool+for+Influencing+Foreign+Policy+Dorothy+E.+Denning&u=a1aHR0cHM6Ly9mYWN1bHR5Lm5wcy5lZHUvZGVkZW5uaW4vcHVibGljYXRpb25zL0FjdGl2aXNtSGFja3RpdmlzbUN5YmVydGVycm9yaXNtLU5ldHdvcmtzQW5kTmV0d2Fycy5wZGY&ntb=1>

Dremluga, R. (2014). Subculture of Hackers in Russia. *Asian Social Science*, 10(18).

<https://doi.org/10.5539/ass.v10n18p158>

Drenning-Blalock, S. (2022). *KillNet\_Threat-Analysis* [Threat analysis]. Quadrant.

<https://quadrantsec.com/blog/threat-analysis-killnet>

Dumbrava, D. (2012). From cybercrime to hacktivism. *Pro Lege Review (Revista Pro Lege)*, 1, 179–192.

Dwan, J. H., Paige, T. P., & McLaughlin, R. (2022). Pirates of the Cyber Seas: Are State-Sponsored Hackers Modern-Day Privateers? *Law, Technology and Humans*, 3(2). <https://doi.org/10.5204/lthj.1583>

European Commission. (2022). *EU sanctions against Russia following the invasion of Ukraine*

[Institutional]. Eu-Solidarity-Ukraine.Ec.Europa.Eu. [https://eu-solidarity-](https://eu-solidarity-ukraine.ec.europa.eu/eu-sanctions-against-russia-following-invasion-ukraine_en)

[ukraine.ec.europa.eu/eu-sanctions-against-russia-following-invasion-ukraine\\_en](https://eu-solidarity-ukraine.ec.europa.eu/eu-sanctions-against-russia-following-invasion-ukraine_en)

European Council. (2023, March 29). *EU response to Russia's invasion of Ukraine* [Institutional].

..Consilium.Europa.Eu. [https://www.consilium.europa.eu/en/policies/eu-response-ukraine-](https://www.consilium.europa.eu/en/policies/eu-response-ukraine-invasion/)  
[invasion/](https://www.consilium.europa.eu/en/policies/eu-response-ukraine-invasion/)

Finnemore, M., & Sikkink, K. (2001). TAKING STOCK: The Constructivist Research Program in

International Relations and Comparative Politics. *Annual Review of Political Science*, 4(1), 391–416. <https://doi.org/10.1146/annurev.polisci.4.1.391>

- Forescout Vedere Labs. (2022). *Killnet. Analysis of Attacks from a Proeminent Pro-Russian Hacktivist Group* [Industry report]. <https://www.forescout.com/blog/killnet-analysis-of-attacks-from-a-prominent-pro-russian-hacktivist-group/>
- GCSC. (2019). *Advancing cyberstability*. <https://cyberstability.org/report/>
- Goode, A. (2015). Cyberterrorists: The Identification and Classification of Non-State Actors Who Engage in Cyber-Hostilities. *Mil. L. Rev.* 223 (2015): 157-197.  
<https://heinonline.org/HOL/LandingPage?handle=hein.journals/milrv223&div=8&id=&page=>
- GoogleTAG. (2023). *Fog of war: How the Ukraine conflict transformed the cyber threat landscape* [Threat analysis]. Google. <https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/>
- Götz, E., & Staun, J. (2022). Why Russia attacked Ukraine: Strategic culture and radicalized narratives. *Contemporary Security Policy*, 43(3), 482–497. <https://doi.org/10.1080/13523260.2022.2082633>
- Grabher, G. (2009). Networks. In R. Kitchin & N. Thrift (Eds.), *International Encyclopedia of Human Geography* (pp. 405–413). Elsevier. <https://doi.org/10.1016/B978-008044910-4.00209-1>
- Guiora, A. N. (2017). *Cybersecurity: Geopolitics, Law, and Policy*. Routledge.
- Hampson, N. C. N. (2012). HACKTIVISM: A NEW BREED OF PROTEST IN A NETWORKED WORLD. *Boston College International and Comparative Law Review*, 35(6), 511. Hampson, Noah C.N., Hacktivism, Anonymous & a New Breed of Protest in a Networked World (September 14, 2011). Boston College International and Comparative Law Review, Vol. 35, No. 6, p. 511, 2012, Available at SSRN: <https://ssrn.com/abstract=1927505>
- Hardy, K. (2010). OPERATION TITSTORM: HACKTIVISM OR CYBER- TERRORISM? *UNSW Law Journal*, 33, 474.
- Hollis, D. B. (2021). A BRIEF PRIMER ON INTERNATIONAL LAW AND CYBERSPACE. *Carnegie Endowment for International Peace*. [https://carnegieendowment.org/files/Hollis\\_Law\\_and\\_Cyberspace.pdf](https://carnegieendowment.org/files/Hollis_Law_and_Cyberspace.pdf)

- Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). *Examining the Social Networks of Malware Writers and Hackers*. 6(1).
- Hurd, I. (2008). Constructivism. In *The Oxford Handbook of International Relations* (p. Pages 298-316). Oxford Academic. <https://doi.org/10.1093/oxfordhb/9780199219322.003.0017>
- Illig, A. T. (2015). *Computer Age Protesting: Why Hacktivism is a Viable Option for Modern Social Activists*. 119.
- Ireland, L. (2022). We are all (not) Anonymous: Individual- and country-level correlates of support for and opposition to hacktivism. *New Media & Society*, 146144482211222. <https://doi.org/10.1177/14614448221122252>
- Jensen, E. T. (2017). The Tallinn Manual 2.0: Highlights and Insights. *Georgetown Journal of International Law* 735.
- Jóhannesson, G. T., & Bærenholdt, J. O. (2009). Actor-Network Theory/Network Geographies. In R. Kitchin & N. Thrift (Eds.), *International Encyclopedia of Human Geography* (pp. 15–19). Elsevier. <https://doi.org/10.1016/B978-008044910-4.00657-X>
- Killmilk, *Podcast Legitimacy Question*. (2022, September 25). [https://vk.com/wall-166346231\\_30239?lang=en](https://vk.com/wall-166346231_30239?lang=en)
- KillMilk, the leader of KillNet. (2022, October 9). *We are an echo of future problems for the States": Killnet announced impending revelations against the West* [Interview]. <https://russian.rt.com/world/article/1059107-killnet-hakery-ssha-razoblachenie>
- Klimburg, A. (2017). *The Darkening Web: The War for Cyberspace* (Reprint edition). Penguin Books.
- Knapp, T. M. (2015). Hacktivism- Political Dissent in the Final Frontier. *New England Law Review*, 49.
- Knappenberger, B. (Director). (2012, October 30). *We Are Legion: The Story of the Hacktivists* [Documentary]. Luminant Media.
- Latour, B. (2007). *Reassembling the Social: An Introduction to Actor-Network-Theory*. OUP Oxford.

- Leuprecht, C., Szeman, J., & Skillicorn, D. B. (2019). The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity. *Contemporary Security Policy*, 40(3), 382–407.  
<https://doi.org/10.1080/13523260.2019.1590960>
- Li, X. (2013). Hacktivism and the first amendment: Drawing the line between cyber protests and crime. *Harvard Journal of Law & Technology*, 27(1), 301–330.
- Liptak, K. (2022, December 21). *5 takeaways from Volodymyr Zelensky's historic visit to Washington* | *CNN Politics*. CNN. <https://www.cnn.com/2022/12/21/politics/takeaways-volodymyr-zelensky-visit-to-washington/index.html>
- Luppici, R. (n.d.). Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research. *Global Media Journal, Canadian Ed.; Ottawa Vol. 7, Iss. 1, (2014): 35-49*.
- Maurer, T. (2018). *Cyber Mercenaries. The state, Hackers and Power* (2018th ed.). Cambridge University Press.
- Milmo, D., & editor, D. M. G. technology. (2022, February 27). Anonymous: The hacker collective that has declared cyberwar on Russia. *The Guardian*.  
<https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia>
- Nye, J. S. (2011). *The Future of Power*. PublicAffairs.
- Paulsen, K. (2021, August 4). *The Benefits, Pitfalls, and Differences of Influencer Marketing Tiers from Micro to Celeb* [Marketing Company]. <https://www.rhythminfluence.com/blog/the-benefits-pitfalls-and-differences-of-influencer-marketing-tiers-from-micro-to-celeb>
- Powers, S. M., & Jablonski, M. (2015). *The Real Cyber War: The Political Economy of Internet Freedom*. University of Illinois Press.

Przetacznik, J., & Tarpova, S. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks* (p. 7). European Union Parliament.

Reardon, R., & Choucri, N. (2012). The Role of Cyberspace in International Relations: A View of the Literature. *2012 ISA Annual Convention San Diego, Ca.*  
<https://nchoucri.mit.edu/sites/default/files/documents/%5BReardon%2C%20Choucri%5D%20012%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf>

RFE/RL. (2017, June 1). Putin Compares Hackers To “Artists,” Says They Could Target Russia’s Critics For “Patriotic” Reasons. *Radio Free Europe/Radio Liberty*. <https://www.rferl.org/a/russia-putin-patriotic-hackers-target-critics-not-state/28522639.html>

Riggi, J. (2023). *HC3 TLP Clear Analyst Note KillNet’s Targeting of the HPH Sector December 2022 March 2023 / AHA* (Analyst Note 20230405120). U.S. Department of Health and Human Services Health Sector Cybersecurity Coordination Center (HC3). <https://www.aha.org/h-isac-green-reports/2023-04-05-hc3-tlp-clear-analyst-note-killnets-targeting-hph-sector-december-2022-march-2023>

Rodrigo Chaves sobre ciberataques: “Estamos preparando un decreto de emergencia nacional.” (2022, April 22). *Delfino*. <https://delfino.cr/2022/04/rodrigo-chaves-sobre-ciberataques-estamos-preparando-un-decreto-de-emergencia-nacional>

Russia-Ukraine crisis: Putin orders military operation in Ukraine – video. (2022, February 24). *The Guardian*. <https://www.theguardian.com/world/video/2022/feb/24/russia-ukraine-crisis-putin-orders-military-operation-in-ukraine-video>

Smith, B. (2022). *Defending Ukraine: Early Lessons from the Cyber War* (p. 29) [Industry report]. 22 June Microsoft.

- Smith, D. (2023, January 27). Exploring Killnet's Social Circles – Radware Blog [Industry]. *Radware*.  
<https://www.radware.com/blog/security/threat-intelligence/2023/01/exploring-killnets-social-circles/>
- 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>
- Tsagourias, N. (2016). Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts. *Journal of Conflict and Security Law*, 21(3), 455–474. <https://doi.org/10.1093/jcsl/krw020>
- UNGGE. (2021). *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. UN General assembly.
- Valeriano, B., & Maness, R. C. (2015). Cyber Conflict and Non-State Actors: Weapons of Fear. In *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (pp. 164–187).  
<http://www.tandfonline.com/doi/full/10.1080/09592318.2016.1151659>
- Wall, D. S. (2012). The Devil Drives a Lada: The Social Construction of Hackers as Cybercriminals. In *Constructing Crime* (pp. 4–18). Palgrave Macmillan, London.  
[https://doi.org/10.1057/9780230392083\\_2](https://doi.org/10.1057/9780230392083_2)
- Wendt, A. (1992). Anarchy is what States Make of it: The Social Construction of Power Politics. *International Organization*, 46(2), 391–425. <http://www.jstor.org/stable/2706858>
- Yildirim, M. (2022). *Dark Web Profile: Killnet - Russian Hacktivist Group - SOCRadar*. SOCRadar® Cyber Intelligence Inc. <https://socradar.io/dark-web-profile-killnet-russian-hacktivist-group/>

## Annex I

**KillMilk, the leader of KillNet. (2022, October 9). *We are an echo of future problems for the States'*: Killnet announced impending revelations against the West** ; Interview with Killmilk accessible at <https://russian.rt.com/world/article/1059107-killnet-hakery-ssha-razoblachenie> . The website cannot be accessed on a normal browser, but can be accessed from the Onion/Tor browser.

**Мы эхо будущих проблем для Штатов»: в Killnet заявили о готовящихся разоблачениях в отношении Запада**

9 октября 2022, 22:29

Основатель группы хакеров Killnet, известный под именем KillMilk, заявил в интервью RT о подготовке разоблачений действий Запада. По его словам, гражданская сетевая инфраструктура США — это «полный ноль для безопасности». KillMilk отметил, что главная цель действий Killnet — «дать отпор врагу».

**— Почему вы решили атаковать американские серверы именно сейчас? Какие конкретно серверы были взломаны? Что с ними происходит сейчас?**

— Америка — это последний оплот наших действий. Мы прошли по всем запланированным странам. Соединённые Штаты хвастаются своей киберподготовкой, но как выглядит это на самом деле и насколько они имеют опыт в ведении кибервойны — вы увидите в ближайшее время с помощью наших действий. Восемь месяцев мы познавали и ломали Европу, тем временем Штаты всё это время готовились к встрече с нами. Мы только начинаем созидать на территории киберпространства Америки. Я добьюсь высшего положения Killnet в мире IT и снесу имя Америки у всех на глазах. Что было взломано сейчас? Это пустяки. Лучше спросите, что будет дальше с информационным полем Соединённых Штатов.

**We are an echo of future problems for the States': Killnet announced impending revelations against the West**

9 october 2022, 22:29

The founder of the hacker group Killnet, known as KillMilk, said in an interview with RT about the preparation of revelations of Western actions. According to him, the civilian network infrastructure of the United States is "a complete zero for security." KillMilk noted that the main goal of Killnet's actions is to "repel the enemy."

**Why did you decide to attack American servers right now? Which specific servers were hacked? What is happening to them now?**

America is the last bulwark of our actions. We went through all the planned countries. The United States brags about its cyber training, but what it really looks like and how much experience they have in cyber warfare is something you will see in the near future with the help of our actions. For eight months we have been exploring and breaking Europe, while the States have been preparing to meet us all this time. We are just beginning to create in the cyberspace of America. I will achieve the highest position of Killnet in the IT world and demolish the name of America in front of everyone's eyes. What has been hacked now? It's nothing. Better ask what will happen next with the information field of the United States.



— **Насколько легко взломать американские серверы?**

— Если говорить о гражданской сетевой инфраструктуре, то это полный ноль для безопасности.

Правительство Америки защищает только свои ресурсы, например Пентагон, ЦРУ и Белый дом.

Это то, что держит имя Штатов. Но гражданский сектор уязвим на 100%, о простых гражданах Америки никто не думает. Значит, будем думать мы.

— **Какова конечная цель ваших действий?**

— Наша основная цель — отпор врагу и мир на земле. Я не хочу, чтобы моя страна имела пассивные обстоятельства в пределах агрессии Европы и США. Мы не будем биться, мы будем бить.

— **Были ли попытки вычислить вас тем или иным способом?**

— Конечно, были и есть по сей день. Я не хочу говорить об этом, всё это очень сложно.

— **Получали ли вы какую-либо информацию (посредством взлома), которая бы скомпрометировала США и/или уличила бы их во лжи? Если да, пожалуйста, приведите примеры.**

— Мы готовим свой огромный пакет доказательств и разоблачения действий США в создании COVID-19. В данный момент идёт завершение собственного расследования по этому делу. Это будет одно из самых громких событий.

Соединённые Штаты причастны к созданию COVID-19. Об этом заявил Killmilk, основатель группы хакеров Killnet.

**- How easy is it to hack into American servers?**

- If we talk about civilian network infrastructure, then this is a complete zero for security.

The U.S. government protects only its own resources, such as the Pentagon, the CIA, and the White House.

This is what keeps the name of the States. But the civil sector is 100% vulnerable, no one thinks about ordinary American citizens. So, we will think.

**- What is the ultimate goal of your actions?**

- Our main goal is to repel the enemy and peace on earth. I do not want my country to have passive circumstances within the aggression of Europe and the United States. We will not fight, we will beat.

**- Were there any attempts to figure you out in one way or another?**

- Of course, they were and are to this day. I don't want to talk about it, it's all very complicated.

**- Did you receive any information (through hacking) that would compromise the United States and / or convict them of lying?**

If yes, please provide examples. "We are preparing our own huge package of evidence and exposure of US actions in the creation of COVID-19. At the moment, our own investigation into this case is being completed. This will be one of the most high-profile events.

The United States is complicit in the creation of COVID-19. This was stated by Killmilk, the founder of the hacker group Killnet

— **Формально ваша деятельность противозаконна. Насколько боитесь последствий?**

— Формально я законопослушный гражданин Российской Федерации. Я не лезу в дела правительства России, я не осуждаю их действий, соответственно, и не совершаю преступления на территории моей родины. Всё, что находится за пределами границы России, — для нас поле битвы, где мы можем реализовать все свои возможности.

— **Какова поддержка среди людей за границей, если таковая есть?**

— У меня огромная поддержка от моих друзей из SOLARIS — это такая же дерзкая и сильная команда из даркнета. Я не знаю, откуда они, но я знаю этих профессионалов очень давно. Благодаря их вниманию в нашу сторону Killnet остаётся на полном ходу. Также наша семья — это наши подписчики из Telegram — являются для нас сильной опорой, за что благодарим их.

— **Как вы думаете, насколько сильно влияют ваши действия на США в целом?**

— Пока что мы просто эхо будущих проблем для Штатов. Пока что! Но CNN уже даёт нехорошие прогнозы. Слава России!

- **Formally, your activity is illegal. How afraid are you of the consequences?**

- Formally, I am a law-abiding citizen of the Russian Federation. I do not meddle in the affairs of the Russian government, I do not condemn their actions, respectively, and I do not commit crimes on the territory of my homeland. Everything that is outside the border of Russia is a battlefield for us, where we can realize all our capabilities.

- **What is the support among people abroad, if any?**

"I have a lot of support from my friends at SOLARIS – it's an equally bold and strong team from the dark web. I don't know where they come from, but I've known these professionals for a very long time. Thanks to their attention in our direction, Killnet remains in full swing. Also, our family - these are our subscribers from Telegram - are a strong support for us, for which we thank them.

- **How much do you think your actions affect the United States as a whole?**

- So far, we are just an echo of future problems for the States. For now! But CNN is already making bad predictions. Glory to Russia!

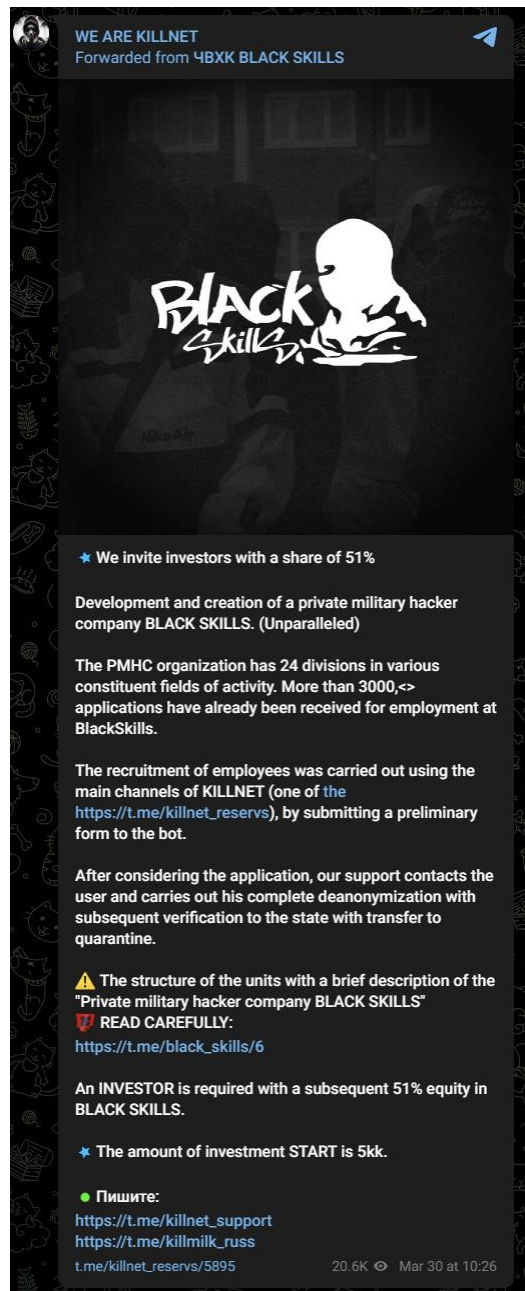
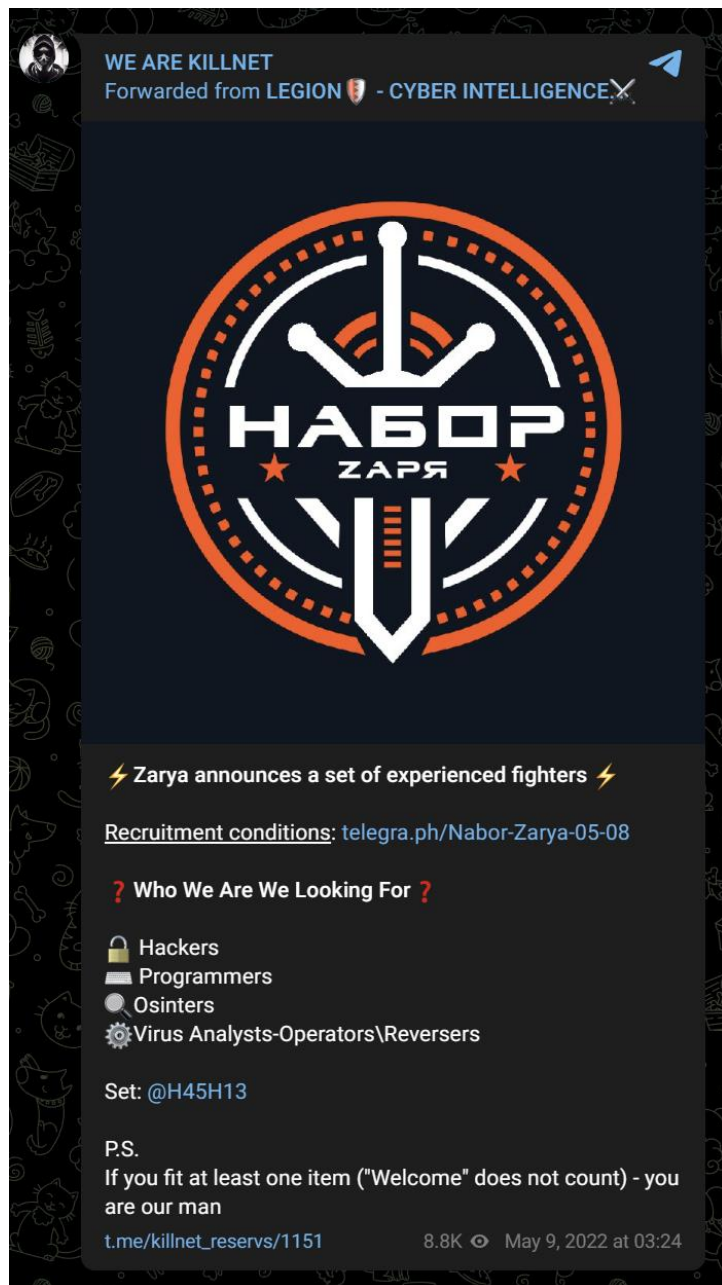


Figure 1 representative graphic for Zarya (Reservs 1151) and Black Skills (reservs/5894)<sup>24</sup>

<sup>24</sup> The original message was translated from Russian to English

Table 1 Top 20 Hashtags

	Hashtag	Translation	Number of use	ER
1.	#killnet	#killnet	38	0.4718
2.	#германияrip	#germanyrip	18	1.6442
3.	#anonymoussudan	#anonymoussudan	17	0.2907
4.	#stopnato	#stopnato	17	1.444
5.	#минобороны	#Ministry of Defense	16	0.196
6.	#россия	#Russia	15	0.1774
7.	#стопнато	#stop	15	0.2624
8.	#украина	#Ukraine	14	0.1742
9.	#anonymous	#anonymous	12	0.6552
10	#уй	Untranslatable – indecent reference	11	2.8961
11	#fucknato	#fucknato	10	0.252
12	#заря	#zarya	10	<b>2.029</b>
13	#дайте сервера киЛлнЕту	#giveserverkillnet <sup>25</sup>	7	0.6453
14	#infinity	#infinity <sup>26</sup>	5	0.1391
15	#й	Untranslatable – indecent reference	5	0.155
16	#демилитаризация	#demilitarization	5	0.155
17	#stopfakeanonymous	#stopfakeanonymous	5	1.0146
18	#stopnazis	#stopnazis	5	<b>3.4196</b>
19	#germanyrip	#germanyrip	4	0.6204
20	#trueanonymous	#trueanonymous	4	1.2232

Saved from: <https://popsters.com/app/dashboard>

<sup>25</sup> Links where people can donate to Killnet

<sup>26</sup> Reference to infinity forum

Table 2 Translated Messages

Ref.	Text	Like s	Vi e w s	Dat e	Url
4	<p>The hacker group Anonymus decided to Hip to the world against the backdrop of a conflict with our brothers from UA Ukrainian!</p> <p>- putting forward their stupid tweets about hacks and DDOS on the server of the Russian Federation</p> <p>- Support for the Naziks of Zelensky and so on.</p> <p>Anons showed us that they are the true whores of the special services of USA 😞</p>	2 4 5	9 2 6 0	2/2 6/2 022	https://t.me/killnet_reservs/4
5	<p>🤖 anons go to bed with the help of DDOS Russian News Observer "RT" and get out of the whole world ...</p> <p>🤖 SMLs from all over the world picking up the news and disseminate information through their infocial resources around the world ...</p> <p>🤖 Ludges reading this news - they give this strength and begin to massively believe in the unnatural power of anonymouses on the network ...</p>	1 5 7	9 6 8 7	2/2 6/2 022	https://t.me/killnet_reservs/5
6	<p>⚡ We are the team of the project Killnet &lt;a href="https://t.me/killnet_channel" class="blue-selection" target="_blank"&gt; https://t.me/killnet_channel &lt;/a&gt; &lt;a href="http://www.killnet.io" class="blue-selection" target="_blank"&gt; www.killnet.io &lt;/a&gt;</p> <p>⚡ Killnet captures world attacks by Anonymous and sends a shame to sleep their official website (&lt;a href = "https: // &lt;a href = "http://www.anonymoushackers.net "class = " blue-selection "target = " "&gt; www.anonymoushackers.net &lt;/a&gt;" class = "Blue-selection" target = "_blank"&gt; https: // &lt;a href = "http://www.anonymoushackers.net" class = "Blue-selection "Target = "_ Blank "&gt; www.anonymoushackers.net &lt;/a&gt; &lt;/a&gt;/) - the site offline is already 78 hours.</p> <p>⚡ Apatio report: &lt;a href="https://check-chost.net/check-report/73b29bfk3c" class="blue-selection" target="_blank"&gt; https://check-host.net/check-report/73b29bfk F3c &lt; /a&gt;</p> <p>⚠ The attack was reflected after 10 days.</p>	2 2 1	1 0 1 4 6	2/2 6/2 022	https://t.me/killnet_reservs/6
13	<p>👉 Enough DDOS Services for Assistance!These resources carry death and Nazi ideology to the masses. To battle ...L7 (http flood) ⚡ &lt;a href="http://&lt;a href="http://www.bratstvo.info" class="blue-selection" tax"&gt; www.bratstvo.info &lt;/a&gt;/"Class = "Blue-Election" target = "_blank"&gt;</p>	1 2 2	1 1 0	2/2 7/2 022	https://t.me/killnet_reservs/13

	<a href="http://www.bratstvo /a/">http:// &lt;a href="http://www.bratstvo /a/"/&gt;</a> ✖ <a href="http://pravyysektor.info/" class="blue-selection" target="_blank">http://pravyysektor.info/ </a> ⚡ <a href="http://naso.org.ua/" class="blue-selection" target="_blank">http://naso.org.ua/ </a> ⚡ <a href="https://unso.in.ua/" class="blue-selection" target="_blank">https://unso.in.ua/ </a> ⚡ <a href="http://berives.org.ua/" class="blue-selection" target="_blank">http://berivets.org.ua/ </a>		9 1		
25	<p>Our answer to the Anonimuses!</p> <p>⚡ The is the appeal of a team of hackers to citizens of the Russian Federation and the CIS countries.</p> <p>- The information is subject to immediate distribution!</p> <p>#Zanas</p>	5 9 5	6 2 9 1 6	2/2 8/2 022	https://t.me/killnet_reservs/25
31	<p>❤ You can support us in crypto format</p> <p>⚡ BTC (Bitcoin) BC1QX9NU6LVLQ5SQU7AFM6SWZCCCC2RYNG8DP9C6D92Z</p> <p>⚡ ETH (Ethereum) 0xc86306527DA67556F23CAFF709D49257221CD6E7</p> <p>⚡ Tether (TRC20) TXOFMF9LVXVPG24XOF34ZM97PHBPT2QQ</p>	3 4 8	4 4 5 9 1	3/1 /20 22	https://t.me/killnet_reservs/31
42	<p>⚡ Doys and respected!</p> <p>There are many fakes on the network with our contacts! Be careful.</p> <p>- Our site Killnet.io</p> <p>- Communication @killnet_support</p> <p>- Channel @killnet_channel</p> <p>- &lt;a href="https://twitter.com/killnet_support" class="blue-selection" target="_blank"&gt;https://twitter.com/killnet_support &lt;/a&gt;</p> <p>- Observer @cyberwar_world</p>	2 0 4	4 0 7 6 8	3/1 /20 22	https://t.me/killnet_reservs/42
67	<p>❤ You can support us in crypto format ⚡ BTC (Bitcoin)BC1QX9NU6LVLQ5SQU7AFM6SWZCCCC2RYNG8DP9C6D92Z ⚡ ETH (Ethereum)0xc86306527DA67556F23CAFF709D49257221CD6E7 ⚡ Tether (TRC20)TXOFMF9LVXVPG24XOF34ZM97PHBPT2QQ</p>	2 4 4	4 4 8 3 6	3/4 /20 22	https://t.me/killnet_reservs/67
199	<p>🔥 Pension of the draw !!!</p> <p>! Get \$ 15 for every 100 reposts of this record!</p> <p>! The most frantic subscriber of our channel receives a rug as a bonus with home delivery!</p> <p>⚡ Prize fund</p> <p>- 5 branded rugs "Wipe your legs from the fucking sector"</p>	5 2 1	1 7 3 1 2	3/2 1/2 022	https://t.me/killnet_reservs/199

	<p>- \$ 1000</p> <p>- A lot of emotions!</p> <p>👤 Rinsing 72 hours</p>				
212	<p>It's been 20 days since the Anonymous threats!</p> <p>How many of you have suffered from these children?</p> <p>Anonymous Poll</p>	3 1 4	1 4 9 5 0	3/2 1/2 022	<a href="https://t.me/killnet_reservs/212">https://t.me/killnet_reservs/212</a>
215	<p>⚠️ ⚠️ ⚠️ Meshens ⚠️ ⚠️ ⚠️</p> <p>! @killnetofficial !</p> <p>! @killnet_zappravdu !</p> <p>! @killnet_zappravdu !</p> <p>❌❌ @killnet_k</p> <p>❌❌ &lt;a href="https://t.me/sad1stxtiktok" class="blue-selection" target="_blank"&gt; https://t.me/sad1stxtiktok &lt;/a&gt;</p> <p>❌❌ &lt;a href="https://t.me/killnet_k_hack" class="blue-selection" target="_blank"&gt; https://t.me/killnet_k_hack &lt;/a&gt;</p> <p>❌❌ @killnet_k_bot</p> <p>❌❌ &lt;a href="https://t.me/killnetofficial" class="blue-selection" target="_blank"&gt; https://t.me/killnetofficial &lt;/a&gt;</p> <p>❌❌ @killnet_k_hack_ru</p> <p>⚠️ We have no bots and other groups except the official channel!</p> <p>Killnet: @killnet_channel</p> <p>Observer: @Cyberwar_world</p>	1 1 9	1 9 7 4 0	3/2 1/2 022	<a href="https://t.me/killnet_reservs/215">https://t.me/killnet_reservs/215</a>
227	<p>👉 Nash protest in support of Kirill Fedorov 👉 "Killnet takes all responsibility for the attack"Attack on the Ministry of Internal Affairs of Latvia ❌ &lt;a href="https://mvd.riga.lv" class="blue-selection" target="_blank"&gt; https://mvd.riga.lv &lt;/a&gt;/ ⚡ &lt;a href="https://check-host.net/check-report/81ec53bkb3e" class="blue-selection" target="_blank"&gt; https://check-host.net/check-report/81ec53BKB3E &lt;/a&gt; ⚡ The attack was stopped after 48 hours&lt;a href="https://check-host.net/check-report/829b4b9k1a2" class="blue-selection" target="_blank"&gt; https://check-host.net/check 1a2 &lt;/a&gt; 👉 For your applications Friends:&lt;a href="https://t.me/cyberwar_world/222" class="blue-selection" target="_blank"&gt; https://t.me/cyberwar_world/222 &lt;/a&gt;</p>	6 8 7	4 6 7 7 2	3/2 2/2 022	<a href="https://t.me/killnet_reservs/227">https://t.me/killnet_reservs/227</a>
244	<p>⚡ Available appeal to the government of Poland from the Killnet team.</p> <p>💠 WAżny Apel do rządu rp z zespołu killnet.</p> <p>👉 Formation is subject to immediate distribution.</p>	1 1 4 9	1 3 6 6 9	3/2 3/2 022	<a href="https://t.me/killnet_reservs/244">https://t.me/killnet_reservs/244</a>
304	<p>⚡ The Polish State Agency of Investment and Trade Paih.gov.pl is evaporated</p>	6 6 9	1 2 7	3/2 7/2 022	<a href="https://t.me/killnet_reservs/304">https://t.me/killnet_reservs/304</a>

	<p>👉 The responsibility for hacking is taken by Killnet.</p> <p>! more than 20 gigabytes of data was pumped out from the Polish protected server.</p> <p>! Self-juicy documents were removed from the archive (fly away for its intended purpose)</p> <p>! We will pretend to personally study part of the data that are on the Pole server.</p> <p>! Scheduled the data &lt;a href="https://mega.nz/file/kmnvnzbr#psBlem0inbrcea02NB3SS814HUNPAAKNCQLZH9UBEVEM" class="blue-selection" target="_blank"&gt; https://Mega.nz/file/kmnvnzbr#psblem0inbrcea02NB3SS814HUNPAAKNCQLZH9UBEVEM&lt;/a&gt;</p>		70		
581	<p>* Board a model with a deep meaning from our designer @alena_des</p> <p>Run the merchants for the most defenseless?</p>	438	7178	4/16/2022	<a href="https://t.me/killnet_reservs/581">https://t.me/killnet_reservs/581</a>
1151	<p>⚡ Zar announces a set of experienced fighters ⚡ Set conditions: telegra.ph/nabor-zarya-05-08 ? We are looking for ? 🗝️ hackers 📝 Programmers 🔍 Osinters ⚙️ Virus analysts-operators \ reversersSet: @h45h13P.S.If you approach at least one point ("welcome" does not count) - you are our person</p>	174	8772	5/9/2022	<a href="https://t.me/killnet_reservs/1151">https://t.me/killnet_reservs/1151</a>
1640	<p>Fake: In Ussuriysk, the military command asks to additionally provide 118 places for the burial of Russian military. This was announced by adviser to the head of the Ministry of Internal Affairs of Ukraine Anton Gerashchenko</p> <p>True: the document that Gerashchenko published is allegedly signed by the commander of the 127th motorized rifle division. But Colonel Tokarev commands her, not Kuzmenkov. The Comdivian addresses the head of the city, despite the fact that the division headquarters is located in Sergeyevka, and not in Ussuriysk.</p> <p>The city administration openly called the letter a fake, they did not receive such a document. The information has already been transferred to the Investigative Committee. Recall that Gerashchenko has already gained the glory of one of the main Ukrainian misinformers, we analyzed his stuffing in detail.</p>	105	6014	5/31/2022	<a href="https://t.me/killnet_reservs/1640">https://t.me/killnet_reservs/1640</a>
1731	<p>Hello hackers 👉</p> <p>Our main channels were blocked by the administration of telegrams for violating the life of our beloved enemies 🐱</p> <p>♦ Nash new channel: @killnet_reservs</p>	8590	5E+05	6/4/2022	<a href="https://t.me/killnet_reservs/1731">https://t.me/killnet_reservs/1731</a>



	<p>♦ Nash Support: @killnet_support</p> <p>If you support our activities on the network, support this entry with a repost! 😊</p>				
1751	<p>⚠️ Guys, this channel I do not know for what purpose and who created. If something is not we &lt;a href="https://t.me/killnetg" class="blue-selection" target="_blank"&gt; https://t.me/killnetg &lt;/a&gt;</p> <p>! Faces !</p>	1 0 1 2	5 4 2 2 7	6/6 /20 22	<a href="https://t.me/killnet_reservs/1751">https://t.me/killnet_reservs/1751</a>
1866	<p>Hello hackers 🙌 There is super news. To date, our botnet zombie network has reached 4.5 million infected devices. Our valiant network engineers are currently upgrading the network to circuit the filtering system "Akamei, Fastly, Incapsula" - under this protection, all the most serious corporations in the world and state institutions "Pentagon, CIA, NATO, and TD" are contained These are the news from Killnet 🦇</p>	3 1 4 6	3 1 9 0 4	6/2 3/2 022	<a href="https://t.me/killnet_reservs/1866">https://t.me/killnet_reservs/1866</a>
2042	<p>Thanks for the donates of the brothers and sisters. Thanks to the boar, Killnet develops its patriotic spirit and skills ❤️</p>	4 6 6 4	5 1 5 9 9	7/2 /20 22	<a href="https://t.me/killnet_reservs/2042">https://t.me/killnet_reservs/2042</a>
2184	<p>Good morning Russia 🙌</p> <p>Perhaps you are familiar with American enterprises that produce weapons. We have chosen the largest of them that has its branches even in Europe, which contributes to convenient logistics for transportation to Ukraine.</p> <p>Once we conducted our special operation against Italy called "Panopticon", I also wrote in the posts that until they understand this word and will be in panic and tension. A panopticon is an emptiness in which everything is visible. This is a psychological effect on a mass of people without the use of any means. On the example of Panopticon, a circle was created, in the middle of the prison there was a tower with holes for a review of the warders for prisoners. All prisoners in this prison behaved freely in order not to turn their eyes off the warders and not get a violation (where they will be entered in a punishment cell and will puss with sticks). But not one of the prisoners could not see the warders in these windows, since the holes in the concrete tower were dark.</p> <p>And were there any warders? 🦇</p> <p>Thus, we gave Italy the grounds for concern, but Italy decided to fuck herself because of the artificially created tension among her population!</p> <p>And we just wrote the text in the posts, but did we really carry out</p>	7 9 3 6	7 3 2 7 9	7/2 1/2 022	<a href="https://t.me/killnet_reservs/2184">https://t.me/killnet_reservs/2184</a>









	<p>attacks? 🦇</p> <p>But we do not open this new front against any country, and this new operation is not using the DDOS system and its escalation! We open a new type of attack and the ability to influence huge corporations for the production of weapons. We will create chaos (this is not a panopticon - these are burning offices and crowds of protests)</p> <p>Subject to the fire 🖱️ Lockheed Martin .....</p> <p>Glory to Russia!</p>				
2214	<p>From this day, the Lockheed Martin defense corporation will be subject to my cyber attacks. Lockheed Martin will be paralyzed! All data of employees of this terrorist company will be published in public access. All Lockheed Martin employees will be persecuted and destroyed around the world! I am against weapons! I am against the trade in death!" I urge all hacker groups to create an escalation in Lockheed Martin production cycles around the world, as well as to disseminate personal information about the terrorists of this company"</p>	5 4 7 2	5 4 8 5 0	8/1 /20 22	<a href="https://t.me/killnet_reservs/2214">https://t.me/killnet_reservs/2214</a>
2428	<p>Vandal Anatol Shalarus states about something there.</p> <p>Killnet costs 24/7 to protect your people !</p> <p>Threatening, this does not mean acting! We are acting. The fraternal people of Moldova, you are not responsible for the actions of your puppet sales government. Ask them a question tomorrow: "Why are Russian evil hackers attack us ???"</p> <p>We will burn evil with hot iron with any means available to us. Each time, politicians threaten our country - we will act and inflict damage.</p> <p>This applies to all countries and politicians who love to speak beautifully publicly.</p> <p>All who are against Russia automatically become enemies Killnet !</p> <p>Moldova - You are next 🔥 🔥</p>	4 8 5 8	4 5 9 3 3	8/2 2/2 022	<a href="https://t.me/killnet_reservs/2428">https://t.me/killnet_reservs/2428</a>
2466	<p>Good morning citizens 🙌</p>	4 6 0 3	6 3 5 0 9	8/2 6/2 022	<a href="https://t.me/killnet_reservs/2466">https://t.me/killnet_reservs/2466</a>
2520	<p>🙌 Today we officially declare war on the Japanese government!</p>	4 5	6 6 3	9/7 /20 22	<a href="https://t.me/killnet_r">https://t.me/killnet_r</a>

	We are Russians... We are killnet ...	6 7	6 8		eservs/252 0
2627	At night, they read the whine in chats and comments and nagging about evacuation and possible mobilization.  Small, cowardly, worthless people. The sense of interpreting men in trousers? I give you skirts?  I have one reason for which I like "mobilization": it is immediately clear who is the Russian brother to me and who put his tongue in the ass and dumped (to the village, in Siberia, on vacation for an indefinite time ITP) or dragged or fucked up. A certain marker, your own, foe.	3 8 5 9	4 5 9 3 8	9/1 3/2 022	<a href="https://t.me/killnet_reservs/2627">https://t.me/killnet_reservs/2627</a>
2829	! City officials and businessmen of the Russian Federation. We need to acquire capacities to continue our activities! We do not receive money from the state and work on a voluntary basis! ⚡ Nazis from Ukraine collect millions of dollars to commit their crimes. And Killnet participants take loans in banks to defend the Russian information field. ! Adres clickable ! BTCBC1QTYJW4WT9AVM0VVVCPKKEWH9TUC2CQ3GMGV6GETH0xeda9832A67711F98E128BCB8F215444DFC273C6B1USDT TRC20TSQGB0X32EKMPFDG1GCM6QWIHEODRACNX ! If you need another address, please write @killnet_support	2 5 1 1	5 1 8 4 2	9/2 5/2 022	<a href="https://t.me/killnet_reservs/2829">https://t.me/killnet_reservs/2829</a>
2858	Hello, my friend! Many dubious actions take place in our country. I understand that enemies behind the cordon are less than inside my homeland. Only some of you understand the specification of our activities. I wrote many times about the types of hacker attacks, about different types of activities of the group of groups! But 90% of you have the provision that a hacker is a very rich and influential person. I would like to explain to you the whole essence of my work. I created a network of computers about 11 months ago. I had a service for the provision of DDOS services. I earned well on destructive activity. But a special military operation in Ukraine began and I closed the Killnet online service in order to use all the forces and opportunities evenly among customers and help Russia - it is impossible! Killnet has turned into hacktivism. Millions of people around the world began to piss into pants with the phrase "These are they, it is Killnet attacking" Why did I do all this? For what I created hundreds of detachments and groups throughout the CIS? For Russia! For my homeland! Who can challenge this? Yes, only yellow-blue pigs!  For half a year, I attracted more than 100 thousand people to Hactivism. I indicated the path for the sound direction - protect the homeland, and scrape off the enemy at its territory! All world newspapers, all world media wrote about my activity. In all the main world news "" Pro - Russian hacker group of Killnet "is strong?	4 2 1 9	6 2 6 0 5	9/2 7/2 022	<a href="https://t.me/killnet_reservs/2858">https://t.me/killnet_reservs/2858</a>

	<p>One person separated the floor of the planet for his homeland! He just left all his black topics in Dark and began to help!</p> <p>Throughout all activities, only a few people helped us financially for which I am insanely grateful to them! But not one official from the Russian Federation, not a single businessman paid his attention to us! Everyone is just a fuck#th!</p> <p>Quote:</p> <p>Once sipping Brendi in an expensive restaurant, one of the Russian millionaires said to his colleagues opposite: Oh, our Russian Killnet hackers bent Lithuania!</p> <p>The end of the quote!</p> <p>Yes, what are we “yours” or what kind of “Russians” are you that you are focusing only on the development of your business and wallet. The floor of the world is waging a war against Russia! Half of the world supplies the Nazis with money, weapons, equipment, etc.</p> <p>And what do you supply - citizens businessmen and officials?</p> <p>About 7 times I crossed over myself and announced the collection of donates from subscribers! And all 6 times all the funds raised are blocking the banking system of Russia, but and the 7th time we were blocked by telegrams :)</p> <p>For what? For the fact that I created a worthy rebuff to enemies? For the fact that we began to respect us? ZBS relations comrades !!!!</p> <p>At the moment, I do not have the opportunity to continue my activities. At the moment, my destructive activity is reduced to only one - there is no finance, there are no servers, but I have more than 5 loans that I took to support Killnet pants! It's ashamed to even write such a thing, but it's more embarrassing for those very people who have great opportunities, but do not want to help us move in the same direction without failures - to victory!</p> <p>Let more altruists like me appear, here's my story, take my experience and fuck the whole world for your people, for Russia ....</p> <p>If suddenly one of the above representatives of the capitalist class woke up a conscience, here is our assembly link: &lt;a href="https://t.me/donate_killnet/28" class="blue-selection" target="_blank"&gt; https://t.me/donate_killnet/28 &lt;/a&gt;</p>				
2870	<p>Good morning cyber mafia! ❤️ Thanks to you, Killnet is staffed and ready to continue!! express my great gratitude for your responsiveness and help! 🙏</p>	3 8 7 9	5 8 4 7 4	9/2 8/2 022	<a href="https://t.me/killnet_reservs/2870">https://t.me/killnet_reservs/2870</a>
2900	<p>14 hacker groups of Russia, today became part of Killnet!</p> <p>- Among them Anonymous Russian.</p>	8 1	5 E +	9/2 9/2 022	<a href="https://t.me/killnet_r">https://t.me/killnet_r</a>

	Killnet is no longer a group! Now Killnet, this is a new global hacker religion in Internet space that protects the interests of the Russian Federation!	4 6	0 5		eservs/290 0
	We are killnet ...				
3029	<p>⚡ Blocking the entire network infrastructure of the largest Bank of America JP Morgan.</p> <p>✗ Platform of institutional liquidity management J.P Morgan Asset Management.</p> <p>✗ InTiral asset management.</p> <p>✗ Chase Connect SM allows customers of medium size to control cash flows and manage banking operations for their business.</p> <p>✗ Paymentech Online coordinates your payment transactions.</p> <p>✗ resource Online places all your data processing data in one place.</p> <p>✗ JP Morgan Markets is a new client platform that will ultimately provide JP Morgan solutions.</p> <p>✗ JP Morgan Access provides specialists in the treasury and investment around the world.</p> <p>✗ JP Morgan Developer - Integration with data and capabilities of the JP Morgan investment bank using unhindered interaction.</p> <p>✗ ABR is a central source of information about American depository receipt.</p> <p>✗ PaymentNet simplifies the administration of all your JP Morgan card programs.</p> <p>✗ JP Morgan Online (USA)</p> <p>✗ JP Morgan Online allows customers to access the residues on their accounts, assets, transactions, extracts and indicators.</p> <p>✗ JP Morgan Online (International)</p> <p>Allows customers of International Private Banking to view and download detailed information about the portfolio and access reports, trading recommendations and performance reports.</p> <p>✗ JP Morgan Online (Asset Management)</p> <p>✗ JP Morgan Online allows customers to access the residues on their accounts, assets, transactions, extracts and results of activity.</p>	5 1 1 4	8 5 4 5 7	10/ 11/ 202 2	<a href="https://t.me/killnet_reservs/3029">https://t.me/killnet_reservs/3029</a>
3137	<p>⚡ Available message to the chief prosecutor of the Republic of Bulgaria - Ivan Grashev - AZ SSM Killmilk, in the lyseto for the organizer for the Khallnet Grape hacker, officially to Zalat's samks for Nazasyano for a special bristles on the brush infrastructure on the Bulgarskoto Korumpyno Government. And to the guardians official! The Prosecutor's Prosecutor for the Republic of Bulgaria Ivan Grashev - Minata Tie! □ I am Killmilk, represented by the organizer of the Killnet hacker group, officially take all responsibility for causing a particularly serious damage to the network infrastructure of the Bulgarian corrupt government. And I declare this officially! The chief prosecutor of the Republic of Bulgaria Ivan Grashev - you go fuck!</p>	5 3 4 3	4 8 7 5 6	10/ 16/ 202 2	<a href="https://t.me/killnet_reservs/3137">https://t.me/killnet_reservs/3137</a>

3764	<p>👋 Friends!</p> <p>➡️ This minute, Killnet includes in its list of enemies all the drug - domestic resources of the Russian Internet.</p> <p>🟡 We gained strength, and are now able to reduce the traffic of drug addicts on sellers to zero! Not without your help, of course comrades!</p> <p>🟢 You will soon receive our telegram of the bot, where you can send the link of any drug resource and inform about the crimes "Wonderers (Video Fixation), suspicious individuals and cars (photo - video)</p> <p>➡️ If the online drug market works in the Russian Federation, which means it is included in the field of view of our like-minded people!</p> <p>😬 A simple formula has long been known for a long time: if you do not have customers, it means losing business! In our case, the loss of Baryg income will be able to stop the development and reproduction of this drug infection in Russia!</p> <p>Glory to Russia. We are killnet.</p>	4 8 8 3	1 E + 0 5	11/ 24/ 202 2	<a href="https://t.me/killnet_reservs/3764">https://t.me/killnet_reservs/3764</a>
3840	<p>Dedicated to the warriors of the 2nd landing company 61 Kirkenes Marine Corps of the Northern Fleet 🤗 On December 31, 1999, at an altitude of 1406 near Kharachoy, 12 naval infantrymen died in a fierce battle with many times superior militants. The marine infantrymen, under the leadership of the platoon commander, Lieutenant Yuri Kuryagin and who had arrived shortly before the location of the captain Alexei Milashevich took an unequal battle. In the first minutes, all officers were killed, and then the command was taken by junior sergeant Vladimir Tatashvili. As a result of a cruel night fight, the death of the heroes fell 12 "black berets", taking away more than 40 militants with them and stopping the bandits at the cost of their life, not allowing them to pass. For the manifested courage and heroism, the marine infantrymen were posthumously awarded the orders, and the platoon commander Lieutenant Y. Kuryagin and junior sergeant V. Tatashvili were awarded the highest award - the title of Hero of Russia, also posthumously.</p>	1 4 4 8	2 8 2 1 8	11/ 27/ 202 2	<a href="https://t.me/killnet_reservs/3840">https://t.me/killnet_reservs/3840</a>
3856	<p>Our friends opened collection for one of the Donetsk boarding schools GOU Donetsk PISH 19</p> <p>To the New Year holidays 🎄 🧸 🧸</p> <p>New Year is difficult to find a more suitable reason to do good deeds, because this is a truly fabulous holiday. Not only children, but adults believe that miracles are possible on this day, and the most pleasant thing is that each of us is able to create them.</p> <p>We invite everyone to join 🤝</p> <p>Together we will give children a holiday ❤️ 🎁</p>	1 1 5 3	1 E + 0 5	11/ 27/ 202 2	<a href="https://t.me/killnet_reservs/3856">https://t.me/killnet_reservs/3856</a>


	All reporting in the form of checks as well as photo and video 🧑 will be published ➡ 2200700401729230 Tinkoff				
4043	 scam  scam  scam  ---- who is signed on our fakes, unsubscribe !!!!!  scam  scam  scam 	6 9 4	3 1 4 8 9	12/ 1/2 022	<a href="https://t.me/killnet_reservs/4043">https://t.me/killnet_reservs/4043</a>
4114	✓ We remind you all!  Sell the huckster: ➡ @narko_stop_bot Pass the pedophile: ➡ @stop_pedophiles_bot Give Milka to beer: ➡ @donate_killnet  We are killnet	1 2 1 9	4 9 2 9 0	12/ 3/2 022	<a href="https://t.me/killnet_reservs/4114">https://t.me/killnet_reservs/4114</a>
4207	🟢 Donat Donat for gifts for the New Year to children's shelters of the Russian Federation. ! Adres clickable ! 🔥 4890494798144549 - Kiwi 🔥 2202206102828063 - Sberbank 🔥 5536914186591297 - Tinkoff 🔥 TONEQAESZO3MMML_CNLGUXY5TBQ3LWWW7PGM76PD9U_PTSWLHULPF 🔥 BTCBC1QRCLC5P3ZN6DZ9AWAWAWAWXJXETX2Y2MTATPALT 🔥 eth0xeda9832A67711F98E128BCB8F215444DFC273C6B1 🔥 usdt trc20TSQGB0X32EKMPFDG1GCM6QWIHEODRACNX 🔥 xmr monero42exW4JPKnm2mgb1vXC8Q66rvsWhx9EVT42UExV3sjvfFHgQXeXzb7act9YNZRepEYJHsFVzFnbCe5jm2DfKGkwwVNz9dqs ! If you need another address, please write @killnet_support 🟢 In accordance with the provisions of paragraph 18.1 of Art. 217 of the Tax Code of the Russian Federation, are exempted from taxation by tax on individuals, income of individuals in monetary and natural forms received from individuals in the order of gift.	8 4 7	3 6 0 7 6	12/ 6/2 022	<a href="https://t.me/killnet_reservs/4207">https://t.me/killnet_reservs/4207</a>
4253	🟢 Spotify, YOUR SERVICE WILL TOWY WORK AFTER PAYMENT - 1 Million Dollars!  Bitcoin: ➡ BC1QTYJW4WT9AVM0VVVCPKKEWH9TUC2CQ3GMGV6G	1 5 5 3	3 5 4 2 6	12/ 8/2 022	<a href="https://t.me/killnet_reservs/4253">https://t.me/killnet_reservs/4253</a>
4278	👏 Like with likes and see how many multinational movement we are! Russian puts - ❤️ Kazakh - 🔥 Belarusian - 🥰 Armenian - 🙏 Gypsy - 🖐️ crests - 😊	1 4 6 6 5 2	3 E + 0 5	12/ 9/2 022	<a href="https://t.me/killnet_reservs/4278">https://t.me/killnet_reservs/4278</a>

	Alien - 🍌 Other fraternal nations -				
4489	❤️ Continue to give the New Year's mood to our kids 🙌 Today, our assistants visited the institution and presented 35 smartphones, bluetooth headphones and sweet gifts! Found only kids, everyone else at school) 🙌 Ram jointly with you Marathon GoodWe are killnet	2 5 2 5	5 8 3 0 7	12/ 22/ 202 2	<a href="https://t.me/killnet_reservs/4489">https://t.me/killnet_reservs/4489</a>
4797	We are the Infinity team and today we get acquainted with the whole world through this news!  Today we have hacked the Central Bloc of the State Tax Service of the United States of America. On our servers there are PASS - access to each 2nd inhabitant of America. We want everyone to understand our presence on the network, we did not come for the separation of your mood, we came to warn specifically towards the American government.  Another step towards the borders of our fraternal peoples, and we will publish the Infinity team 198 million lines IRS.gov to public access!  We support our friends from Killnet, and are ready to go with them shoulder to the shoulder to the end!  Glory to the Slavic nation! Glory to the fraternal and holy of our history! Glory to Belarus and Russia!  Infinity Hackers by - <a href="https://infinity.ink" class="blue-selection" target="_blank"> <a href="https://infinity.ink">https://infinity.ink</a> </a>	2 5 0 1	3 0 2 2 9	1/1 6/2 023	<a href="https://t.me/killnet_reservs/4797">https://t.me/killnet_reservs/4797</a>
4894	All khak groups supporting the mission of the Russian Federation in the fight against the Nazis - we launch the hashtag #Germanyp to verify the participation in the full -scale cyber attack on Germany!  Write just hashtag #Germany on your channel! And take part in holy revenge for our ancestors!	2 6 6 9	4 9 2 8 5	1/2 4/2 023	<a href="https://t.me/killnet_reservs/4894">https://t.me/killnet_reservs/4894</a>
5231	☀️ The Killnet team is announcing a Start attack on all NATO divisions.  🔵 The blow to the Ramstein database, I'm waiting for yours) <a href="https://check-chost.net/check-report/ea0cddfk5a3" class="blue-selection" target="_blank"> <a href="https://check-host.net/check-report/ea0cddfk5A3">https://check-host.net/check-report/ea0cddfk5A3</a> </a>	1 7 6 6	2 3 7 1 8	2/1 2/2 023	<a href="https://t.me/killnet_reservs/5231">https://t.me/killnet_reservs/5231</a>
5681	👋 Well, my little ones, it's time and talk ...Here I once thought at my leisure, about how it all began. But after 7 months I had to reduce our ranks from a useless crowd and traitors. And what do we have in the end now? - We have excellent experience, and most importantly "independence". We have acquired close and friendly contacts with serious people from those very bowels of the Internet as the support of our mission. I am talking about different groups of hactivists and cyber	9 9 8	3 2 3 4 4	3/1 2/2 023	<a href="https://t.me/killnet_reservs/5681">https://t.me/killnet_reservs/5681</a>



	<p>criminals. 🔥 99% RU Communist Party hates us for political views and attitude to his - but we are enough for the same 1% who will stand next to us, and will give the fuck@LU to any ill -wishers. Therefore, I am proud of this, and boldly write about it. So ... 🇷🇺 I launch a new structure of hactivism according to RU community. It will not be just a movement with your ideas. This will be an organizational machine with its own laws and goals, with discipline and order. 24 units with 100% synchronization among themselves. A single block with a hot line 24/7 for receiving appeals and orders. It will be a "private military hacker organization Black Skills" in translation (black skills) ⚠️ submit an application for consideration of your candidacy for work in the Black Skills CHCK Filling out the form below! 🟢 The form is clickable 🟢 - Full years- Knowledge of program languages- Political conviction- The composition of the family- Are you ready to undergo a full ownership for hiring in a CVC?- Your Nationality- Knowledge of English- Education- Work in the state service- Military service- Your username in telegrams ⚠️ 👁️👁️👁️ Send the form to @killmilk_support_bot in this bot and wait for feedback.</p>				
5691	<p>⚠️ The structure of units with a brief description of the Black Skills Private Military Haker company 📄 No. 1 - Support Department (supply and equipment of units with everything necessary for work in the organization - PC, special equipment and other application devices) 📄 No. 2 - Intelligence unit (collective work on pre -information production - Osin, DOX and other tools and methods of intelligence) 📄 No. 3 - public communication department (reception and search for orders around the world, work with the media) 📄 No. 4 - Scientific Center (development and study of any methods of impact on the goal - via the Internet) 📄 No. 5 - personnel department (registration, checking and reception at the "CSHK Black Skills" 📄 No. 6 - Security Service (supervision of all departments of the CVC, full rights, admission to any information) 📄 No. 7 - a group of pentesters (testing for penetration (jarg. Pentest or pentesting) - a method for assessing the safety of computer systems or networks by means of modeling the attacker of an attacker, have admission to orders) 📄 No. 8 - Operational group (equipped detachment of 8 people to rapidly respond to an urgent request to the CVC, 12 hours of "1 Group - 4 people" are under the supervision of the security service), only trusted PTC employees from any units. 📄 No. 9 - Analytical Center (work on information obtained, a forecast of situations, the creation of proposals for the development of CVC, monitoring cyber incidents and large -scale incidents in the world) 📄 No. 10 - a control group (tracking the implementation of the assigned tasks, monitoring. The group is under the supervision of the "Security Service Service of the CVHK") 📄 No. 11 - assault detachment (has a direct contact with the aim of eliminating it, the detachment has a separate hot line with the CHFK operator for an operational request or information transmission) 📄 No. 12 - Department for Work with Investors (creation and acceptance of proposals from investors, conclusion of contracts,</p>	1 0 3 6	3 0 7 5 0	3/1 3/2 023	<a href="https://t.me/killnet_reservs/5691">https://t.me/killnet_reservs/5691</a>

	<p>accounting) ☐ No. 13 - Accounting (has access to procurement information, has the right to request information from the commander of any detachment, the introduction of financial control over all the CSHK, the accrual of wages, statistics) ☐ No. 14 - training center (training of mercenaries after registration, distribution by detachments) ☐ No. 15 - Technical Department (team from IT specialists for maintenance and escorting the FECHK units) ☐ No. 16 - sabotage detachment (creating misinformation and escalation to anywhere in the world with the use of network technologies, destructive activity) ☐ No. 17 - Operational group AlphaM65 (information and psychological operations in enemy countries, exposing stuffing, preventing - unauthorized meetings, rallies, demonstrations, processions, prevention of terrorist attacks - cheekbones jacket, matchmaking, luminous and more. ☐ No. 18 - the Black Skills Network battalion (consists of black hackers, obeys only the head of the organization) ☐ No. 19 - department for combating scammers on the Web (acceptance of applications, tracking crypto - transactions, collecting information, establishing criminals, transferring information to law enforcement agencies) ☐ No. 20 - Business Center (development of CVC, work on advertising) ☐ No. 21 - the main archive (collection of information on the performance of the tasks of the CSHK, the collection of publicly accessible and private information related to the drain of databases from around the world) ☐ No. 22 - Knowledge Center (every 30 days a mercenary attends lessons and lectures to improve his position) ☐ No. 23 - landfill (place for testing new means of impact on the network, work under curators No. 4, No. 14 of the department) ☐ No. 24 - Black Skills Chief Headquarters 📧 apply for a job at the CHKHK_____</p>				
5754	<p>🔥 infinity.ink 🔥</p> <p>Greetings, forum users! Today I want to say a few words about our forum.</p> <p>First of all, I want to say that the forum is apolitical. No war, no conflict based on disagreements between governments. This is a place, a kind of saloon, where all the inhabitants of Darknet can relax. Someone wants to discuss controversial topics. Someone wants to sell the loot, service, etc. Make peace and money, not war!</p> <p>Second. The forum is only 2.5 months, a lot will be added ... the first in line is the DSTAT service. I want to invite all hackers (rus, ua, us, ch). Let's create a good future. The war will end, and work in a darknet is never.</p> <p>Sincerely, the Infinity team!</p>	4 5 1	2 5 5 6 5	3/2 0/2 023	<a href="https://t.me/killnet_reserves/5754">https://t.me/killnet_reserves/5754</a>
5895	<p>☀️ I am the investors with the shared participation of 51%Development and creation of a private military hacker company Black Skills. (Has no analogues)The organization of the CSHK has 24 divisions in different</p>	2 9 2	2 0 5	3/3 0/2 023	<a href="https://t.me/killnet_r">https://t.me/killnet_r</a>

	<p>components of activity. More than 3,000 applications have already received for hiring in BlackSkills. A set of hired employees was carried out using the main channels of Killnet (one of <a class="blue-selection" href="https://t.me/killnet_reservs" target="_blank">https://t.me/killnet_reservs</a>), by serving the preliminary form to the bot. After consideration of the application, our support is associated with the user and conducts its full deanonymization with subsequent verification in the state with quarantine transfer. ⚠️ The structure of units with a brief description of the Black Skills Private Military Hacker company <a class="blue-selection" href="https://t.me/black_skills/6" target="_blank">https://t.me/black_skills/6</a> An investor is required with the subsequent shared participation of 51% in Black Skills. 🌟 Summa of investment Start 5kk. 🟢 write: <a class="blue-selection" href="https://t.me/killnet_support" target="_blank">https://t.me/killnet_support</a> <a class="blue-selection" href="https://t.me/killmilk_russ" target="_blank">https://t.me/killmilk_russ</a></p>		8 1		eservs/5895
5898	<p>This is a fantastic fatal coincidence</p> <p> t.me/killnet_mirror</p>	7 6 0	2 2 3 2 3	3/3 0/2 023	<a href="https://t.me/killnet_reservs/5898">https://t.me/killnet_reservs/5898</a>
5967	<p>🚩 Office proposal Dark School - Killnet. Hello my friend, my name is Killmilk! Today we first decided to release official training from our Killnet team, and share with you our experience that we gained for the difficult 2022! We examined the world web, we attacked enemies on the network, we were mistaken but studied our mistakes, we developed and moved on! I bring to your attention 9 courses of the hottest models for conducting a professional cyber in war or increasing the balance of your wallet! - ddos (17/4) - Google Adwords Arbitration - Fakes (creation, promotion, profit) - Carding (Europe, America) - Osint/Deanon (Cyber Intelligence) - pegasus (spy software for Android/iOS) - Social engineering - Methods of Cyber War (psychology and action on the subconscious of any participant in the World Wide Web) - Diversion on the Web (Methodology) 🔥 Read completely   Apply for training 🟢 Learning is available in four languages (Russian, English, Spanish, Hindi) RU @dark_school_killnet_ru GB @dark_school_killnet_eng ES @dark_school_killnet_es IN @dark_school_killnet_in</p>	5 6 2	3 1 6 4 1	4/4 /20 23	<a href="https://t.me/killnet_reservs/5967">https://t.me/killnet_reservs/5967</a>
6001	<p>200,000 votes "The destruction of NATO on the network!" - Leave your vote, help Killnet make the right choice! "We know the way and have the tools to inflict serious damage on NATO online. It remains only to ask the people of the Russian Federation about it</p>	2 3 0 9	4 2 4	4/6 /20 23	<a href="https://t.me/killnet_reservs/6001">https://t.me/killnet_reservs/6001</a>

6008	<p> We Attacking Israel, Because of What They Did to PalestineWE Hope EVERYONE Attacks, You Can Start Attacking Now   We attack Israel due to what they did with PalestineWe hope that everyone is attacking, you can start attacking now</p> <p>● &lt;a href="https://&lt;a href="http://www.lal.com" class="blue-selection" target="_blank"&gt; www.elal.com &lt;/a&gt; "class = "blue-selection" target="_blank"&gt;https://&lt;a href="http://www.elal.com" class="blue-selection" target="_blank"&gt;www.elal.com&lt;/ a&gt; &lt;/a&gt;/   El Al Israel Airlines is the National Airline of Israel   El Al Israel Airlines - Israeli National airline. ● &lt;a href="https://&lt;a href="http://www.i24news.tv" class="blue-selection"&gt; www.i24news.tv &lt;/a&gt; "class "Blue-Election" target = "_blank"&gt; https: // &lt;a href="http://www.i24news.tv" class="blue-selection" target="&gt; www.i24news.tv &lt;/ a&gt; &lt;/a&gt;/   It is an International News Television Channel Based in Israel   This is an international news television channel based in Israel. ● &lt;a href="https://tau.ac.ac.il" class="blue-selection" target="_blank"&gt; https://tau.ac.ac.il &lt;/a&gt;/   TEL AVIV University   Tel Aviv University ● &lt;a href="https://&lt;a href="http://www.mossad.gov.il" class="BLUE-SELECTION"&gt; www.mossad.gov.il &lt;/A. &gt; "Class =" Blue-Election "target =" "_blank "&gt; https: // &lt;a href="http://www.mossad.gov.il" class="collue-selection" taret="_blank"&gt; www .mossad.gov.il &lt;/a&gt; &lt;/a&gt;/   Israel's National Intelligence Agency   National Intelligence Department of Israel ● &lt;a href="https://&lt;a href="http://www.rambam.org &gt; "Class =" Blue-Election "target =" "_blank "&gt; https: // &lt;a href="http://www.rambam.org.il" class="blue-selection" target="_blank"&gt; www .rambam.org.il &lt;/a&gt; &lt;/a&gt;/   Rambam Hospital, is a Teaching Hospital   Hospital Rambam, training hospital ● &lt;a href="https://&lt;a href="http://www.clalit.co.il" class="blue-selection" target="_blank"&gt; www.clalit.co.il &lt;/a &gt; "Class =" Blue-Election "target =" "_blank "&gt; https: // &lt;a href="http://www.clalit.co .clit.co.il &lt;/a&gt; &lt;/a&gt;/   It is the Largest of the Four State-Manded Health Service Organizations in Israel   This is the largest of the four state medical organizations of Israel. ● &lt;a href="https://&lt;a href="http://www.rail.co.il" class="blue-selection" target="_blank"&gt; www.rail.rail.co.il &lt;/a &gt; "Class =" Blue-Election "Target =" "_blank "&gt; https: // &lt;a href="http://www.rail.co.il" class="blue-selection" target="_blank"&gt; www .rail.co.il &lt;/a&gt; &lt;/a&gt;/   ISRAEL RAILWAYS LTD., Is the Main State-Code Railway Company Responsight for All Rail Transportatio   ISRAEL RAILWAYS LTD. - The main state railway company, which is responsible for all railway transportation. ● &lt;a href="https://&lt;a href="http://www.checkpoint.com" class="blue-selection"&gt; www.checkpoint.com &lt;/a&gt; "class" class " "Blue-Election" target = "_blank"&gt; https: // &lt;a href="http://www.checkpoint.com" class="blue-selections kaya" target="&gt; www.checkpoint.com &lt;/ a&gt; &lt;/a&gt;/   Software Company Known for Its Firewall and VPN Products. Founded in Israel   The software development company, known for its firewalls and VPN</p>	8 5 9	3 4 9 6 5	4/7 /20 23	https://t.me/killnet_reservs/6008
------	---	-------------	-----------------------	------------------	-----------------------------------

	products. Founded in Israel ● <a href="https://<a href="http://www.leumi.co.il" class="blue-selection" target="_blank">www.leumi.co.il </a> "Class =" Blue-Election "target =" _blank "> https:// <a href="http://www.leumi.co.il" class="blue-selection" target="_blank"> www .leumi.co.il </a> </a>/  Bank Leumi is an israeli bank   Bank Leumi is an Israeli bank. ● <a href="https://<a href="http://www.iaa.gov.il" class="blue-selection" target="_blank">www.iaa.gov.il </a> "Class =" Blue-Election "target =" _blank "> https:// <a href="http://www.iaa.gov.il" class="blue-selection" target="_blank"> www .iaa.gov.il </a> </a>/  Ben Gurion Airport   Ben-Gurion Airport ● <a href="https://<a href="http://www.tin.tv" class="blue-selection" target="_blank">www.tin.tv </a> "class = "Blue-Election" target = "_blank"> https:// <a href="http://www.tin.tv" class="blue-selection" target="_blank"> www.tin.tv </ a> </a>/   The Israel Network is a Private International Television Network   The Israel Network is a private international television network. ● <a href="https://<a href="http://www.jpost.com" clas="blue-selection" tax">www.jpost.com </a> class = class = class = "Blue-Election" target = "_blank"> https:// <a href="http://www.jpost.com" class="blue-selection" target="_blank"> www.jpost.com </ a> </a>/   Israeli Newspaper   Israeli newspaper#Anonymoossudan#Killnet				
6060	I could not help but do this - and registered 150 hacked posts of NATO employees on the gay gay portal in Kyiv and Moldova 🤖	4 2 9 5	2 8 4 8 1	4/1 0/2 023	https://t.me/killnet_reservs/6060
6063	⚡ 50 seats for \$ 249  ✓ Registration in Dark School by Killnet  🔥 Chospital Channel Killnet	6 6 7 6 9	9 1 4 8 5	4/1 0/2 023	https://t.me/killnet_reservs/6063
6201	✓ 1 - group (set end) beginning on May 10 🔥 2 - group (set started - cost of training \$ 249) ⚡ Registration in Dark School by Killnet	4 0 4	3 2 5 0 0	4/1 6/2 023	https://t.me/killnet_reservs/6201
6277	If I had connections in the Kremlin, I would have long ago opened the whole world, since I would have financing ... Joe Tidy, I once told you that you are listening to the stories of pigs that are disinfectors. Just like your work on the BBC film is complete shit. Why are you focusing on victims of violence? 😊 I understand, they are sorry for you, but not us!	1 0 4 7	2 2 3 9 8	4/1 9/2 023	https://t.me/killnet_reservs/6277
6339	Hi, I am tired of waiting for help from state or businessmen from the Russian Federation.The servers were again the European bastards eliminatedTuned lousy, mesh fell ...Dear thieves, dealers, black businessmen, exchangers and other people with money - pay attention to the old Milka, and provide him with help in the reorganization of strength and continuing the destructive of the enemies network! 🔥	1 6 8 9	3 1 6 3 4	4/2 0/2 023	https://t.me/killnet_reservs/6339

	Donat / help 🌟 Question - why does Milk do not earn, all hackers are millionaires. Answer: While everyone is earning, I spend all my time with benefit not for profit, probably therefore Killnet is the most loud group in the world, but also the poorest. Our altruism will not bring us to good ... Everything is difficult, and my patience is the end of friends ... If I burn out, you will find out about this first. Hugged everyone!				
6671	GLORY TO RUSSIA !!! ❤️ RU  30k hearts of this post!	7 9 6 2 9	1 0 8 4 4 6	5/1 6/2 023	<a href="https://t.me/killnet_reservs/6671">https://t.me/killnet_reservs/6671</a>
6948	🔔 72 hours ago, three chapters of hacker groups from Russia and Sudan held another meeting in the Darknet parliament, and came to a general decision:  ⚡ Settlement No. 0191  - Today we begin to impose sanctions against European banking transfer systems SEPA, IBAN, Wire, SWIFT, Wise.  Translation^  × 72 Hours AGO, Three Heads of Hacker Groups from Russia and Sudan Held a Regular Meeting in the Darknet Parliament, and Came to a Common Decision:  × Solution No. 0191  - Today We are Starting to Impose Sanction on the European Banking Transfer Systems Sepa, IBAN, Wire, SWIFT, Wise.  We are killnet 🤖	2 2 9 6	1 0 1 8 4 9	6/1 6/2 023	<a href="https://t.me/killnet_reservs/6948">https://t.me/killnet_reservs/6948</a>