Categorizing Cyber Activity Through an Information-Psychological and Information-technological Perspective, Case Ukraine

Harry Kantola
Finnish National Defence University, Helsinki, Finland

harry.kantola@mil.fi

Abstract: Russian approach to warfighting includes an informational facet. Western hemisphere usually treats cyber activity as a tool similar to traditional warfighting tools such as rifles, artillery and tanks, whereas the Russian approach has an informational and narrative stance to the whole conflict. Placing information in the focus, switches the cyber activity to serve either an informational-psychological or an informational-technical approach. Examining the activity from this non-conventional trait and correlating it to other activities during the execution, the study highlights the coordination of kinetic and non-kinetic actions in an altered manner. In this article I am examining cyber activity through the terms of information-psychological and information-technological approach to form an understanding of Russian or Russian supported activities in cyber space before and during the Ukraine crisis. This will recognize types of cyber activity connected to actions in the physical environment. Actions identified are categorized and placed in a matrix created on psychological and/or technical clout. From this matrix groups of activities are scrutinized in correlation to other activities to expose possible narratives or underlying themes. The study relies on a variant of Grounded theory and is selected to elude from examine technical methods and actions. The observed timeframe is for the first study from 2021, well before the current hot phase, until summer 2022. This article is the first part of a two-stage study, where the first part examines cyber activity through the terms of information-psychological and information-technological approach. The second study places the previous findings in correlation to actions, reactions and mitigation activities to find out how defensive measures were relevant or if the outcome were result of something else than deliberate defensive (cyber-)activities. Throughout the larger study, the underlying hypothesis is that there is a larger coordination of cyber activities than acknowledged related to the ongoing crisis.

Keywords: Information-Psychological Warfare, Information-Technological Warfare, Cyber Warfare, Cyber Operation Compilation, Cyber Operations

1. Introduction

1.1 Motivation

Technological phenomena and activity within cyber space related to the ongoing Ukraine crisis has been studied in large extent, especially by technical cyber security companies and think-tanks. Common for most of them, is that they focus on observing *how* the activity was carried out technically. A few have explored possible correlations between kinetic activity and cyber events. An example of this is the special report from Microsoft, *Defending Ukraine: Early Lessons from the Cyber war* (Microsoft, June 2022), which exemplifies some activity, where a direct link between different attacks in a physical and artificial environment can be demonstrated.

In addition, purposes and coordination of activities has not been academically scrutinized. Present reports and studies make assumptions either that there is no real cyber activity correlated to the activities in the physical world, since there have not been any large-scale breakdowns in Ukrainian cyber space (Lewis, 2022) or that the sophistication of the attacks is not high enough. Therefore, the assumption is that cyber has not played a large role in the crisis.

Through this study, I aim to prove the above stated assumption incomplete and to present, that there has been an attempt to coordinate activities in cyber space with activity in the physical world. Moreover, I will highlight how different types of activity has been utilized during the observed timeframe. The fact, that the known cyberattacks has not had a major breakthrough has more to do with the overall poor conduct of the atrocities overall than with due to lack of attempt within cyber space.

1.2 Purpose, scope and structure

This research examines cyber activity from an informational context, and not from a technical categorization, as analysis of cyber incidents are usually conducted. Main focus is why observed activities have been performed, not how it technically was conducted.

The research area has been limited to observe activities that are related to the Ukraine crisis and has further more been narrowed down in this paper to include activities just before the main assault took place in February 2022 until late summer 2022. This includes activities that relate to the crisis also in late 2021. For the sake of clarity, a few examples from 2015-2021 have been included in the material.

The structure of the article is as follows. First, I will justify the use of the chosen theory and tools. By this, I will introduce an alternative way of looking at activities in cyber space compared to traditional western approach. This is also to present an introduction to the Russian way of thinking regarding the utilizing cyber activities as part of warfare. Finally, the analysis of the material is considered and conclusions are drawn from the processed material.

2. Used theory

The ambition with this study is to examine the how cyber activity has played a role in the atrocities related to the ongoing war in Ukraine, explicitly observed by a non-western approach dividing the phenomenon in informational-psychological and information-technical category.

To elude from a purely technical approach I have chosen to use Grounded Theory as a tool to categorize the events in an appropriate way for the study. The purpose is not to examine the technical actions, but to strive for the purpose and connection to other ongoing activities during the aggression. Therefore, it is important to fade the normal technical approach and catalogue the actions differently.

The purpose of Grounded Theory is to develop theoretical explanations about a specified phenomenon. (Creswell, 1998). Through this inductive analysis the product, patterns, themes and categories, would emerge out of the data rather than being imposed on them prior to data collection and analysis. The focus is to gather data from a variety of sources. As the data is scrutinized by the researcher, themes are expected to emerge (Bowen, 2006). A central principle of data analysis is a constant comparison of the data with other similar groups of data to find similarities and differences. Through this reoccurring comparison trends and patterns are being refined. The used method described is deviated from Strauss and Corbin original axial coding (Bryman 2008).

2.1 Grounded Theory as a tool

As stated earlier, the aim for this study is to find patterns and correlations on actions taken in cyber space and other activity specially to find larger groups of activities that can then be compared to Russian military doctrine and concepts. Emerging groups, patterns and categories are compared to each other and finally compared how these groups and categories correlate to the categorization of information-psychical and information-technological thinking.

Accordingly, to the theory, coding the data, regrouping and then scrutinizing the data produces concepts and categories. The following outcome would be a hypothesis regarding the observed phenomenon, when the data is further processed. (Bryman, 2008). The found concepts and categories have been of importance to be able to compare, correlate and observe relations to actions in the physical domains.

2.2 Suitability of grounded theory in observing cyber activity

Regrouping conducted activities obscures the technical details and makes it easier to find out the method of attack. For the sake of this study, it is not necessary to study these methods in the detail, but rather when these are used during military operation phases. Thus, the important thing is to find out types of action, when those are used and how it correlates to doctrine and actions in other domains.

Even though Grounded theory is originally a sociological approach, it has proven to be suitable to extract the needed information for this analysis. This study has found indicators of used concept and existing categories and created a preliminary hypothesis regarding the ways and how activities have been conducted in coordination with regular warfare in the Ukrainian crisis during 2022.

3. Alternative approach to coordinate cyber activity for state purposes

Russian information security doctrine (Доктрина информационной безопасности Российской Федерации [Doktrina], 2016) and lower regulations and guidelines in accordance with it determines how Russia handles cyber space. A notably difference in terminology is that in Russian language there is no “cyber space”. Instead, the terminology uses “information space” as the closest equivalent (Ristolainen 2017).

Keir Giles states that there is a difference in how cyber capabilities are treated in western and eastern approaches to information and cyber activities. Whereas western society threats cyber activity as a separate function, or nowadays as a domain, Russian consider these activities as just tools in the larger information ecosystem. (Giles, 2016). This consideration applies also for Chinese categorization. (Thomas, 2004)

The phenomena which are considered to take place in cyber space, is referred to as "information space" in Russian terminology. These activities are further divided into information-technical and information-psychological strands in Russian thinking. (Giles, 2016). "*Warfare in information space can be information-technical, when informational technical systems are objects of influence in cyber space, or it can be information-psychological, when the adversary tries to influence a person's mind, his or her moral and mental world, political opinions and ability to make decisions*" (Kari, 2019)

Russia had an attempt to introduce "electronic Russia" already in 2001, (Thomas 2010), but the lessons learnt in the Russian-Georgian conflict 2008 reshaped the approach to the traditional approach. The conflict pinpointed the need to better control the informational aspect of war and coordinate the activities with the traditional domains. This includes the control of information-psychological and information-technological undertakings in external, internal and military activities. (Thomas, 2010)

Russian military doctrine practically dates back to 2010 (Security Council of the Russian Federation), although minor changes were made to it in 2014. In accordance to these doctrines and follow up guidelines, Russia has to be able to inflict in both cognitive and physical space. Combining the doctrine and guidelines for the military with the existing information doctrine highlights, that the Russian approach is divided in two; information-psychological and information-technological approach.

It has been taken into account, that the Russians do not have actual cyber-doctrine. Instead, there is an information doctrine that includes also issues, which "in western terminology" would be described as actions in cyber space. Examining the activities in Ukraine through the alternative approach might give a better understanding on how and why activities has been Implemented.

4. Case Ukraine

4.1 Dataset

Cyber activity has not been widely discussed during the conflict. This might partly be related to the fact that there have not been any large-scale knock-on effects on human lives whereas the conventional activity has. (Lewis, 2022). Additionally, there were a critical uncovering of malicious cyber activity just in the last minute before the attack, when Mandiant discovered the wiping malware aimed at Ukraine. (Mandiant, 2022)

Up until summer 2022 there has been reported far beyond 300 separated cyber incidents in the Ukrainian crisis (Microsoft, June 2022). In this study I have limited the examination to focus on the year 2022, including activities in January and February before the conventional attack was initiated. The material has been extended to with some relevant additions from the timeframe starting with 2015 to 2021 due to their direct linkage to the actions in 2022. The dataset has been amassed from different databases, such as national Cert databases, and cybersecurity companies' factsheets or bulletins. These have been supplemented with relevant news releases (see references).

Data from far beyond 350 separate reports regarding cyberattacks has been filed per technical indicators. These has then been regrouped and merged to form attack type categories, especially to remove duplicate reports, where the same event is reported under a different name. A typical example of this is the HermeticWiper (SentinelLabs), aka. FOXBLADE (Microsoft), aka. KillDisk (Mcafee), malware, that has different name depending on which cybersecurity company is reporting it. The coding process produced a set of 90 categories, which have then been subordinated to constant comparison and further more correlation examination to both actions on the ground and relation to existing military doctrine.

The number of attacks carried out indicates that the use of cyber has been incorporated as a tool in the toolbox. Missions have been conducted both to inflict on critical infrastructure and command and control functions as well as affecting accessibility to information and media outlets.

4.2 Examination of the data

The material shows that there Is a specific approach where some types of attacks relate to information-technical actions connected to events in the physical world and some types of attacks are meant to affect the cognitive aspects of the victim or victims. These strikes wary pending on type of target and the desired effect.

In order to examine how the attacks have been carried out in different categories, I have divided the material into a grid that is divided first of all into information-technical and information-psychological divisions and

secondly in an assessment of their severity. Picture 1 will depict a snapshot of how the material has been categorized and regrouped accordingly to the used grounded theory. The picture shows activities early

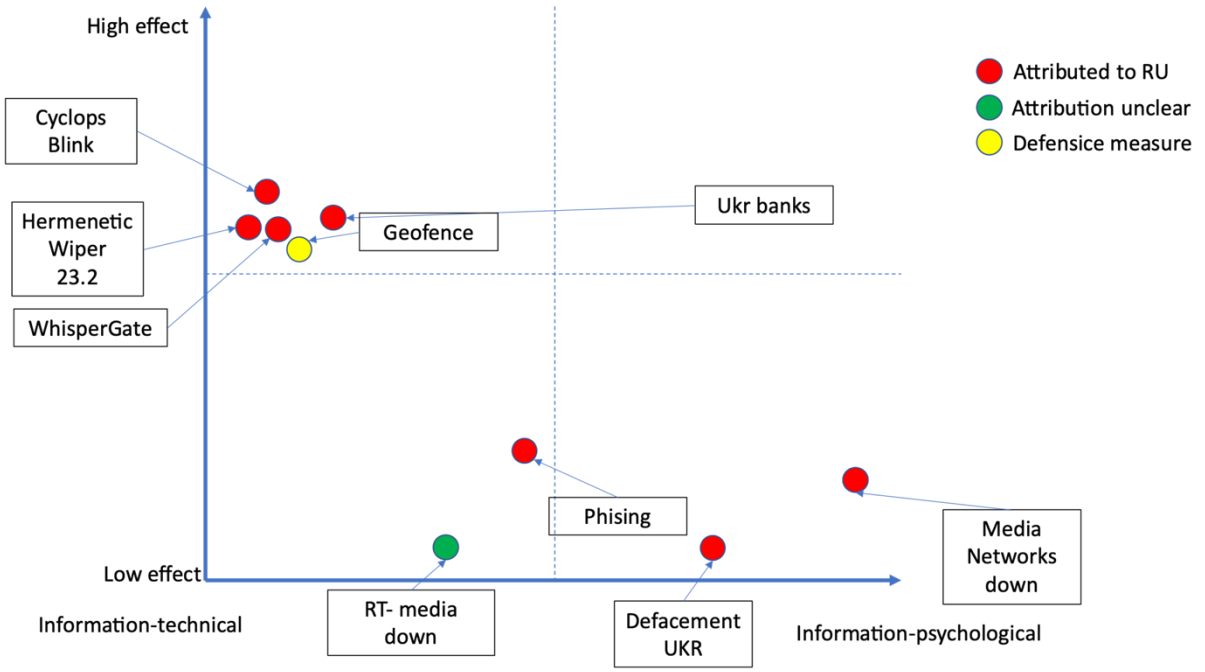


Figure 1: Snapshot of the categorization work

This material has after categorization then been examined from different perspectives. The only common unitary factor, is the division into information-psychological and information-technological classes in the processing of the materials.

The scale and criteria used in this study is entirely created for this purpose. The upper limit of the scale us set to the level 5. This level describes a potentiality for total destruction of the system or impact on the decision making or society. On the other end, nuisance is given the level 1. The scale in between represents different levels of potential impact. An impact level 2 represents effects, that have a short time impact or effects that can be repaired and corrected within a reasonable time. Typical and normal resilience measures should ward of these types of attacks. Impact level 3 represents attacks that potentially requires defensive actions or counter measures. Severity of the potential impact rises above minor damage either in the system or within the situational awareness or decision cycle. Finally, an impact level 4 describes attacks that potentially can severely harm actions, operations, decision making and/or the society in at a length or requires substantial efforts to tackle. All examined attacks are given a level based on their potential effect or outcome, regardless if the attack were successful or not.

Examining the events by severity, it can be noted that information-technological attacks have often been able to create more serious ramifications. Although not all attacks achieve a high penetration into systems, these have had an impact on the comprehensive situation in the area. As a rule, information-technical cases achieve a higher level of effectiveness, although not all of them exceed the level of "teasing".

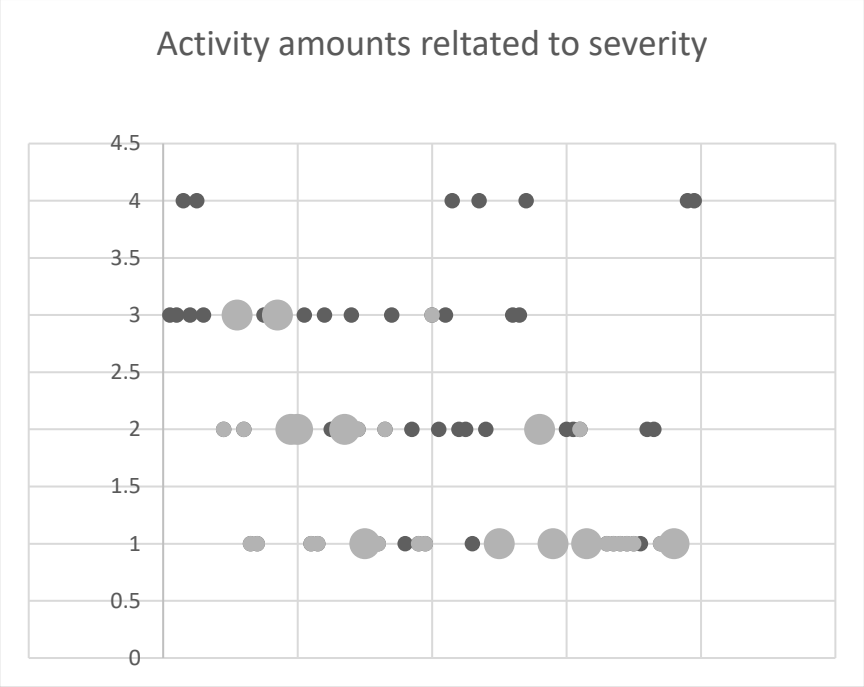


Figure 2: Categorizing the material according to severity. Dark dots represent information-technical activity and light grey dots information-psychological. Size of dot represent amounts of activity.

At the same time, I note that information-psychological events tend to be carried out more frequently. Information-psychological attacks are also larger in number and also targeting more actors at the same time. Thus, as the scope of targets are easily increased, the severity does not increase nor have an impact on the target audience as a whole.

I also note, that the information-technological events took place earlier in the crisis and the information-psychological actions relatively evenly throughout the observed timeframe. This can be identified more clearly in picture 3, where the line presents the relation between the two observed categories.

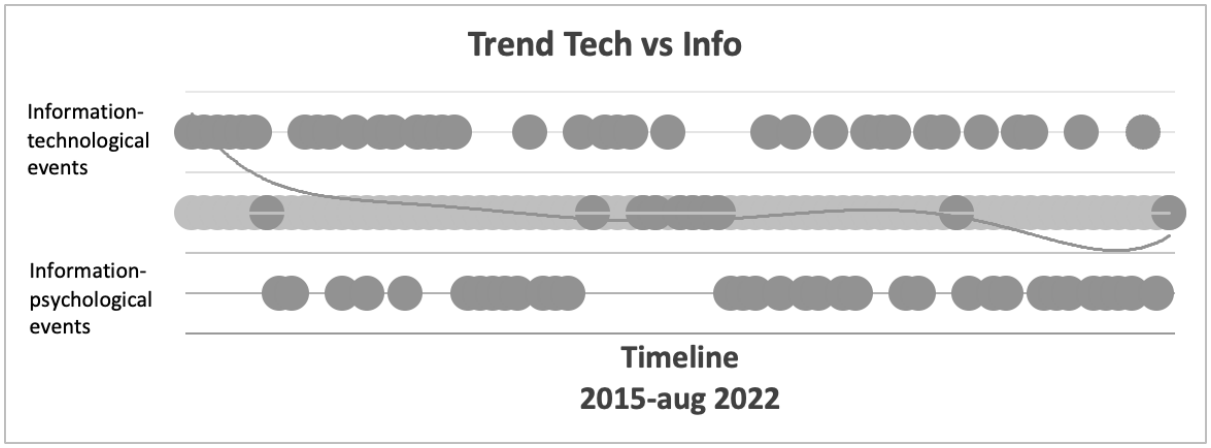


Figure 3: Information-technical and information-psychological activities on a timeline.

The preliminary assessment also suggests that as while the technological level shifts towards less sophisticated targets, it also seems to change to a greater extent opportunistic approach. This seems to be true for both information-technological and information-psychological objectives.

5. Conclusions, discussions and further work

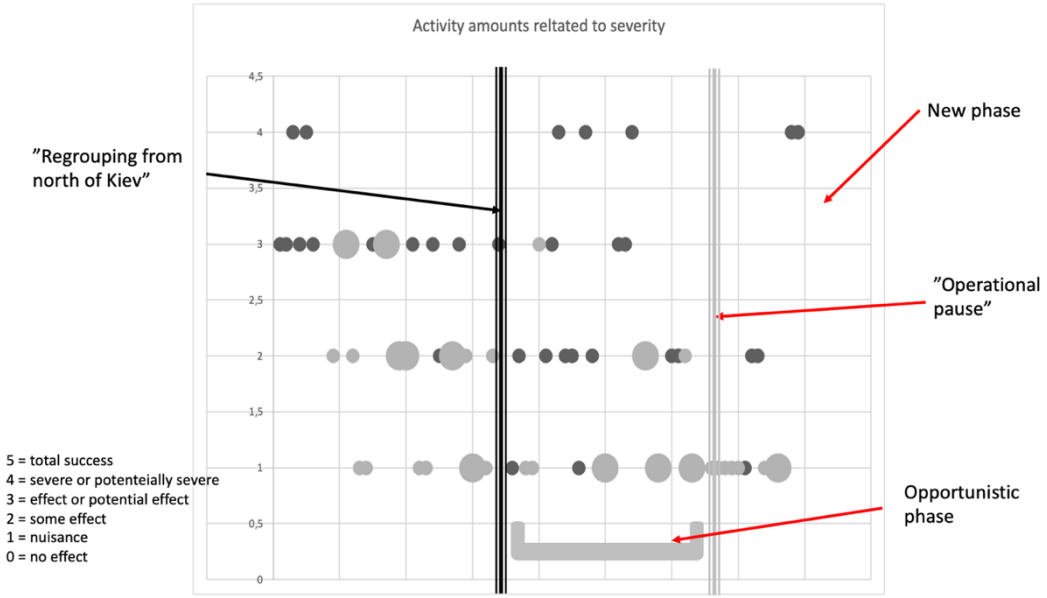
5.1 Conclusions

The result of the study shows first of all, that there was originally a plan to combine kinetic and non-kinetic action. The non-kinetic actions were aimed at both information-technical systems, that is the function of the system, and psychological, that is the cognitive level of citizens and governmental actors through cyber space. Higher in severity and more technical approach were conducted early in the conflict while actions towards the cognitive domain were more of a supporting role. Attacks conducted in the information-psychological sphere were to add on to the fog of war and ability to have a clear picture of what is going on. In addition, the information-psychological approach aimed apparently to change the mindset of the citizens, after a victorious short kinetic battle.

Secondly, it can also be seen from the material that while the actions in the physical world did not work out as planned, the correlating planned actions towards technological systems were (or in fact, tried to be) carried out in preplanned manner. The fact that a large part of the activity was repelled, does not have to do with the events in the physical world, but more with that many attack vectors had been tried before or the malware were found in due time by defenders.

Thirdly, when the planned activity in the traditional domains and cyber space did not work, the activity shifted from information-technical towards information-psychological activity. At the same time the attacks seem to be more and more carried out opportunistically. The data shows also that within the information-psychological niche there were attacks conducted accordingly to premade plan and ad-hoc new attempts performed when the progress with the boots on the ground did not proceed as planes.

Furthermore, the activity in cyber space coincides with the activity on the ground. When the Russians had to rearrange (withdraw) from the northern attack direction and to establish what is called in military terminology an operational pause, there were also an “operational pause” in the activity in cyber space. The above-mentioned analysis and information are depicted in picture 4.



Picture 4: Operational phases of land battle correlated with cyber activity.

After the initial attack and the first phase of the war the connection and coordination regarding attacks in the physical world and in the cyber domain decline. There are still attempts to create more value combining actions, but these are only sporadic incidents. Also new information-technological attacks have been conducted after an extensive preparation phase. These are less in amount and less in coordination with other actions taken. Common for both approaches, is that the severity has gone down over time. Only some sporadic attempts have had a severe potentiality, especially after an extensive preparation phase at the very end of the observed timeframe.

5.2 Discussion

Examining the material gives a suggestion that the planned and effective actions were not conducted in planned time. Possibly due to changes in plans and timing. This led to exposure and disclosure. A large amount of the more severe information-technical attacks could be ward off in the nick of time, due to the actions the dormant malwares conducted while waiting for the right time. The preliminary analysis suggest that the malwares were too early in place and did not get permission to launch as planned.

The material indicates also that there has been a strategic masterplan to combine the action in the kinetic and non-kinetic world. The fact that it didn't succeed has more to do with the struggle in real life and that the war has not gone after plan, than with poor coordination between the domains. This shows that coordinating activities in real time challenging.

Examined cases demonstrates that Russian approach has a clear division in information-technical and information-psychological activities. The Russian forces tries to utilize both approaches. Each of the methods has a role within the military actions and has to be included in the military strategies and operations. As stated before, the challenge is to be in due time.

Actions in cyber space, preparation, tests and footholds, can give indications on upcoming activities in physical world. As seen in this case study, activities in late 2021 and January 2022 gave indications away. The same giveaway came when malwares started to beacon for permission to act. All these gave the defenders tools to repel forthcoming attacks.

At this stage, it is too early to draw final conclusions. It seems to be indications that traditional doctrine is implemented in cyber- (information) actions and goal settings. Activities had been planned in conjunctions with assessed advance on the ground.

5.3 Further work

Elaboration, regarding how much effort were placed on changing citizens mindset versus affecting havoc on systems needs further examination. Fast and deliberate initial attack on systems and a shift towards cognitive influence has still to be proven, even though the material indicates a correlation.

By expanding data set to include pre 2014 activities, there should be possibilities to find out how much of indications and warnings, mitigation techniques and defense measures were put in place before the actual attack in February. This analysis would also bring to light how much of same techniques, malwares, and vulnerabilities were utilized or reused. For this purpose, the timespan should be expanded to include data from the years 2013 to 2022.

Found data indicates also that by analyzing selected timeframes, there might be possibilities to find reasons why imminent attacks were revealed. However, this information requires further investigation and study.

References

Avertium (2022), *CISA Warns of renewed Russina Threat as new Activity is seen in Ukraine,* Avertium, https://www.avertium.com/blog/cisa-warns-of-renewed-russian-threat-new-activity-seen-in-ukraine

Black, D. (March, 2022), *Hero hackers claim to have breached Belarusian weapons firm,* Cybernews, https://cybernews.com/news/hero-hackers-claim-to-have-breached-belarusian-weapons-firm/

Black, D. (April 2022) *Ukraine left reeling by 'zombie' cyberattacks*, Cybernew,s https://cybernews.com/cyber-war/ukraine-left-reeling-by-zombie-cyberattacks/

Bowen, G. A. (2006) *Grounded Theory and Sensitizing Concapts,* Ingernational Journal of Qualitative Methods.

Bryman A. (2008) *Social research methods (third edition)*. Oxford University Press, New York, ISBN 978-0-19-920295-9

Cert-UA (2022), *Новини, (Eng. news), Ukraine state, https://cert.gov.ua/articles*

Creswell, J. W., (1998) *Qualitative Inquiry and Research Designe: Chooose Among Five Traditions.* Sage Publications. London

Corfeld, G. (2022), *Ukraine shrugs off mass govt website defacement as world turns to stare at Russia,* https://www.theregister.com/2022/01/14/ukraine_cyberattack_gov_websites_defaced/

Doktrina (2016) *Doktrina infomatsionnoi bezopasnosti Rossiiskoi Federatsii, [Доктрина информационной безопасности Российской Федерации]*, (information security doctrine of the Russian Federation), http://kremlin.ru/acts/bank/41460/page/1 viewed 9 august 2022,

ESET Research, (April, 2022) *Industroyer2: Industroyer reloaded,* WeLiveSecurity, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

ESET Research (May, 2022), *Sandworm uses a new version of ArguePatch to attack targets in Ukraine, WeLiveSecurity,* https://www.welivesecurity.com/2022/05/20/sandworm-ukraine-new-version-arguepatch-malware-loader/

Fisher, D., (2022), *Sandworm group deploying new Cyclops Blinck malware*, Duo Security – Dechiper, https://duo.com/decipher/sandworm-group-deploying-new-cyclops-blink-malware
Gatlan, S. (September, 2022) *Google says former Conti ransomware members now attack Ukraine*, Bleeping computer, https://www.bleepingcomputer.com/news/security/russian-sberbank-says-it-s-facing-massive-waves-of-ddos-attacks/amp/
Geller, E. (2022), *Ukraine prepares to remove data from Russia's reach,* Politico https://www.politico.com/news/2022/02/22/ukraine-centralized-its-data-after-the-last-russian-invasion-now-it-may-need-to-evacuate-it-00010777
Giles, K. (2016) *Handbook of Russian Information Warfare,* NATO Defence College Fellowship Monograph Series 9 ISBN978-88-96898-16-1
Github (2022). Github.com https://github.com/Orange-Cyberdefense/russia-ukraine_IOCs/pulse
Greenberg, A. (2022) *Destructive Hacks Against Ukraine Echo Its Last Cyberwar,* https://www.wired.com/story/russia-ukraine-destructive-cyberattacks-ransomware-data-wiper/
Hacker News, (2022), *Russian Hackers APT28 and UAC-0098 Target Ukraine Again,* https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/
Haskell-Dowland, P. (2022), *As Russia wages cyber war against Ukraine, here's how Australia (and the rest of the world) could suffer collateral damage*, The Conversation; academic rigour, journalistic flair, https://www.helpnetsecurity.com/2022/02/24/cyber-attacks-ukraine/
Holland, S., Pearson, J:, (2022) *US, UK: Russia responsible for cyberattack against Ukrainian banks*, https://www.reuters.com/world/us-says-russia-was-responsible-cyberattack-against-ukrainian-banks-2022-02-18/
Jones, D. (2022). *Botnets, data wiping malware spread as Ukraine incursion begins*, https://www.cybersecuritydive.com/news/botnets-data-wiping-malware-ukraine/619362/
Jonsson, O. (2019) *Russian information warfare and its challenges to international law,* Routledge Handbook of war.
Kari, M. J., (2019), *Russian Strategic Culturi in Cyberspace; Theory of Strategic Culture; a tool to explain Russia's Cyber Threat Perception and Response to Cyber Threats,* Dissertations 122, Jyväskylä University
Kundalyja, D. (2022) Ukrainian hacker leaks Conti ransomware internal chats after gang sides with Russia, Computing, https://www.computing.co.uk/news/4045605/ukrainian-hacker-leaks-conti-ransomware-internal-chats-gang-russia
Leonard B. (2022), *Continued cyber activity in Eastern Europe observed by TAG*, https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/
Libicki, M. (2007), *Conquests in Cyberspace, National Security and Information Warfare*, Rand Corporation, Cambridge University Press. ISB*N* 978-0-521-87160-0
Lewis, J. A. (2022), *Cyber War and Ukraine*, Centre for Strategic and International Studies, report on: https://www.csis.org/analysis/cyber-war-and-ukraine
Mackie, K. (2022) Microsoft Ukraine Report Warns of Coming Zero-Day Exploits, Redmond, https://redmondmag.com/articles/2022/04/27/microsoft-ukraine-report-warns-of-coming-zero-day-exploits.aspx
Malwarebytes lab, (2022), *Cobalt Strikes again: UAC-0056 continues to target Ukraine in its latest campaign,* https://www.malwarebytes.com/blog/threat-intelligence/2022/07/cobalt-strikes-again-uac-0056-continues-to-target-ukraine-in-its-latest-campaign
Microsoft Corporation (April 2022), *Special Report Ukraine: An overview of Russia's cyberattack activity in Ukraine.* https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
Microsoft Corporation (June 2022), Defending Ukraine: Early Lessons from the Cyber War, *https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK*
Milmo D. (2022), *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
National Cyber Security Center (UK), (2022), https://www.ncsc.gov.uk/news/uk-organisations-encouraged-to-take-action-around-ukraine-situation
Petkauskas V. (2022) *Eurovision cyberattack: pro-Russian hackers declared 'war' on ten states,* https://cybernews.com/cyber-war/eurovision-cyberattack-pro-russian-hackers-declared-war-on-ten-states/
Ristolainen, M. (2017): *Should 'RuNet 2020' be Taken Seriously? Contradictory Views about Cybersecurity between Russia and the West*, Journal on Information Warfare, vol. 16, no. 4, 113-131
Schneier, B. (2022) Microsoft Issues Report of Russian Cyberattacks against Ukraine, https://www.schneier.com/blog/archives/2022/04/microsoft-issues-report-of-russian-cyberattacks-against-ukraine.html
Sharma, Y. (2022) *Anonymous leaks 15,600 new emails from GUOV I GS via DDoSecrets*, https://www.thetechoutlook.com/news/technology/anonymous-leaks-15600-new-emails-from-guov-i-gs-via-ddosecrets/
Smith, B. (2022), *Defending Ukraine: Early Lessons from the Cyber War,* Microsoft, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/
Socradar.io (2022) *What you need to know about Russian Cyber escalation in Ukraine; The Second Wave of Cyber Attacks on Ukraine: Deadlier than the First Wave.* https://socradar.io/what-you-need-to-know-about-russian-cyber-escalation-in-ukraine/#The-Second-Wave-of-Cyber-Attacks-on-Ukraine-Deadlier-than-the-First-Wave

Symantec (February 2022), *Ukraine: Disk-wiping Attacks Precede Russian Invasion*, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia
Symantec (April 2022), *Shuckworm: Espionage Group Continues Intense Campaign Against Ukraine*, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-intense-campaign-ukraine
Telychko, V. (2022), AgentTesla Information-Stealing Malware Delivered in Cyber-Attacks on Ukrainian Government Entities, SOCPRIME, https://socprime.com/blog/agenttesla-information-stealing-malware-delivered-in-cyber-attacks-on-ukrainian-government-entities/
Thomas, T. L. (2004) *Russian and Chinese information warfare: theory and Practice*, Presentation, https://apps.dtic.mil/sti/pdfs/ADA467510.pdf)
Thomas T.L (2010) *"Russain Information warfare Theory: The consequences of August 2008" in s Blank and Weits (eds.) The Russian military today and tomorrow,* 2010.
Toulas, B (April, 2022), *Russian hacktivists launch DDoS attacks on Romanian govt sites,* Bleeping computer, https://www.bleepingcomputer.com/news/security/russian-hacktivists-launch-ddos-attacks-on-romanian-govt-sites/amp/
Toulas, B. (May, 2022). *Russian Sberbank says it's facing massive waves of DDoS attacks,* Bleeping computer, https://www.bleepingcomputer.com/news/security/russian-sberbank-says-it-s-facing-massive-waves-of-ddos-attacks/amp/
Toulas, B. (June, 2022) *Russian govt hackers hit Ukraine with Cobalt Strike, CredoMap malware*, Bleeping computer LLC, https://www.bleepingcomputer.com/news/security/russian-govt-hackers-hit-ukraine-with-cobalt-strike-credomap-malware/
Treloar, S. (2022). *Russian Hackers Target Norway in Latest Volley of Cyber Attacks*, Bloomberg, https://www.bloomberg.com/news/articles/2022-06-30/russian-hackers-target-norway-in-latest-volley-of-cyber-attacks
YouTube, (2022), https://www.youtube.com/watch?v=dwbDMnEraO0, (at 5 min 23 sec)
Zetter, K. (2022), *Russia Began Setting Stage for Cyberattacks Against Ukraine a Year Ago,* Zero Day, https://zetter.substack.com/p/russia-began-setting-stage-for-cyberattacks?s=r
Zorz, Z. (2022) *Cyber attacks on Ukraine: DDoS, new data wiper, cloned websites, and Cyclops Blink,* HelpNetSecurity, https://www.helpnetsecurity.com/2022/02/24/cyber-attacks-ukraine/