INFINITY

IMMERSE. INTERACT. INVESTIGATE.

Policy Brief

Cyber Threat Overview: Armed Conflict in Ukraine

DISSEMINATION LEVEL PUBLIC

PARTNER

CyberPeace Institute

AUTHOR

Florent Bitschy

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 883293. The content of this document represents the view of the authors only and is their sole responsibility. The European Commission does not accept any responsibilty for any use that may be made of the information it contains.

Cyber Threat Overview: Armed Conflict in Ukraine

Cyber Threat Overview: Armed Conflict in Ukraine[1]

One of the goals of the CyberPeace Institute is to establish if there are any links between cyberattacks against entities to geopolitical or economic events. These events include what is happening in regards to the war physically in Ukraine, but also in other countries, whether it be the announcement of economic sanctions against Russia, military support for Ukraine and/or political statements from government officials.[2]

1.General overview

Since the February 2022 Russian military invasion of Ukraine, the CyberPeace Institute has been documenting cyber incidents in the context of the Russian-Ukrainian conflict. This includes incidents in Ukraine, the Russian Federation and other countries notably those targeting and/or impacting civilians, civilian objects (including private companies) and infrastructure ensuring the delivery of essential services to civilians. The data is available through the Cyber Attacks in Times of Conflict Platform[1] #Ukraine.

As of 9 April 2023, the Institute has documented 1593 cyberattacks and operations, averaging 22.8 attacks per week, and as many as 93 different threat actors. In the case of Ukraine, the Institute documented 368 attacks against the country since January 2022. In the case of the Russian Federation, there have been 250 cyberattacks since January 2022.

The Institute also tracks cyberattacks against non-belligerent countries that support Ukraine, as there is a clear geopolitical link to the conflict. Thus, there have been 975 cyberattacks documented against non-belligerent countries (44 countries so far), the vast majority of these being DDoS attacks conducted by hacktivist collectives.

No.	Country	Incidents
1.	Poland	176
2.	Latvia	96
3.	Germany	83
4.	USA	83
5.	Lithuania	82
6.	Czech Republic	51
7.	Estonia	49
8.	UK	45
9.	Japan	28
10.	Sweden	26

1 https://cyberconflicts.cyberpeaceinstitute.org

2. Breakdown by quarters

The Institute has published three quarterly reports detailing activity in the context of the war. Each of these reports summarizes cyberattack activity, highlights the trends, emerging issues and notable threat actor activity during its respective period in Ukraine, the Russian Federation and non-belligerent countries. To give a better overview of the cyber threat landscape in regards to the war, the major findings of each report will be presented in chronological order.

Q3- July to September 2023[3]

This was the first quarterly report published by the Institute. In this report, the institute not only summarized cyber activity from the beginning of January 2022, but also highlighted activity during the third quarter of 2022 (from July to September).

Ukraine

The Institute documented 87 of the attacks were specifically during the third quarter, representing a 248% increase in activity compared to the previous quarter. Key Findings from Q3:

- Public Administration remained the most targeted sector in Q3, followed by Media in second place, and ICT/Financial tied for third.
- DDoS attacks accounted for 71% of all incidents, followed by Malware (8%).
- Hacktivist collectives accounted for 80% of all incidents.
- Notable threat actor activity:
  - Five campaigns were attributed to Russian state-sponsored threat actors
  - The increase in DDoS activities against Ukrainian entities was likely related to Russian media coverage of Russian hacktivist collectives. Media interviews with the groups' leaders portrayed them as "defenders of Russia" and "patriots", likely causing increased awareness and participation in the groups' activities. Those collectives rely in part on the participation of the general population. Examples from the report included People's CyberArmy and KillNet.

Russia

The Institute documented 48 incidents impacting 12 sectors in Q3, there was a 27% decrease in incidents compared to the previous quarter. Key Findings from Q3:

- Most targeted sectors included Public Administration, Financial Sector, Administrative/Support, ICT, and Transportation.
- Cyberattacks: 79% DDoS , 13% Hack and Leak, 2% Defacement and the remaining unknown.
- Hacktivist collectives accounted for 34% of all incidents against entities in the Russian Federation but there was a 93% decrease in activity compared to Q2 of the hacktivist collective Anonymous and its affiliates.
- Most notable threat actors included the IT Army of Ukraine and Haydamaki.

Other Countries

The Institute documented 141 incidents impacting 19 sectors in Q3, representing a 177% increase in attacks against states outside the two belligerent states compared to the previous quarter. Key Findings from Q3:

- DDoS attacks accounted for 91% of all incidents.
- While Public Administration was the most targeted sector in Q1 and Q2, the Transportation sector was targeted the most in Q3, with an increase of 220% compared to Q2. Nevertheless, Public Administration remained a high-priority target for threat actors conducting cyberattacks against entities in countries outside the two belligerent states. The Financial sector saw a 380% increase in cyberattacks in Q3 compared to Q2.
- Hacktivist collectives accounted for 85% of all incidents. There was a decrease in the activities of the most active threat actors by the end of Q3 (such as KillNet and NoName057(16)).
- Most notable threat actor was NoName057(16).

Q4- October to December 2023[4]

Ukraine

The Institute documented 71 incidents impacting 16 sectors in Q4, representing an 18% decrease in incidents compared to the previous quarter. This decrease was driven by a decline in substantiated incidents targeting Ukrainian entities by pro-Russian hacktivist collectives. Key Findings from Q4:[41]

- DDoS attacks accounted for 87% of all incidents.
- The most targeted sector in Ukraine was the Financial sector which saw a 117% increase compared to Q3. Public administration experienced a 52% decrease in attacks. The Institute noted increased attacks against the Transportation, Trade, and Administrative/Support sectors.
- Two campaigns were attributed to Russian State-sponsored threat actors, Sandworm and Gamaredon.
- Hacktivist collectives accounted for 91% of all incidents targeting entities in Ukraine.
  - 72% decrease in incidents attributed to the People's CyberArmy.
  - 89% increase in incidents attributed to Anonymous Russia.
  - 240% increase in incidents attributed to NoName057(16).
- KillNet announced the creation of a forum that would unite all pro-Russian threat actors.

Russia

The Institute documented 26 incidents impacting 11 sectors in Q4, representing a 46% decrease in incidents compared to the previous quarter, marking a second consecutive quarter of declining incidents against entities in the Russian Federation. Key Findings from Q4:

- The ICT sector was targeted the most. The Public administration was the second most targeted sector; attacks against the Financial sector continued to persist.
- For the first time since the start of the conflict, the Institute detected several attacks claimed by pro-Russian threat actors against Russian entities, and disputes between different pro-Russian hacktivist groups.
- While cyberattacks against Russian entities decreased by 46%, the impact of the incidents was more pronounced than those in other countries. The personal information of more than three million Russian citizens and millions of lines of additional personal information emerged in the public domain due to several hack and leak operations.

Other Countries

The Institute documented 239 incidents impacting 16 sectors in Q4 against entities in nation-states that are not the two belligerent states and noted a 369% increase in attacks. Key Findings from Q4:

- DDoS attacks accounted for 99% of all incidents.
- Entities in 27 different countries were targeted in Q4, an increase of 42% compared to Q3. In Q4, the most targeted entities by proRussian threat actors were in Poland (70 incidents), Latvia (32 incidents), and the United States of America (22 incidents).
- The Public administration was the most targeted sector in Q4, with a 204% increase compared to Q3, continuing the trend set in Q1 and Q2 of 2022. The Transportation sector remained a high-priority target for pro-Russian threat actors, with an increase of 31% in the incidents compared to Q3. The third most targeted sector was the Administrative/Support sector, with a 200% increase in attacks against it. The Financial sector saw a 20% decrease in attacks compared to Q3.
- Notable threat actor activity included NoName057(16) and Anonymous Russia.

Q1- January to March 2023 [5]

Ukraine

- 104 incidents against entities in Ukraine with DDoS attacks accounting for 88% of all incidents.
- The threat actors that were the most active in targeting Ukrainian entities were the hacktivist collectives People's CyberArmy (99), NoName057(16) (40) and Anonymous Russia (26). Sandworm (19) and DEV-0586 (12) have had the most attacks attributed to them among Russia's state-sponsored threat actors.
  - Five incidents have been attributed to Russian state-sponsored threat actors including three campaigns attributed to Sandworm (attributed to Russia's foreign military intelligence - GRU) and two cyberattacks attributed to DEV-0586.
- Top 5 targeted sectors impacted: • Public administration (81) • Financial (43) • Media (34) • ICT (33) • Transportation (18) & Energy (18).
  - 12 Ukrainian non-profit organizations were targeted in 5 DDoS attacks or campaigns in February 2023.

Russia

- 65 incidents against entities in the Russian Federation.
- The most active threat actors conducting attacks against Russian entities were the IT Army of Ukraine (59), the global hacktivist collective Anonymous (49) and Anonymous Italia (37).
- Top 5 targeted sectors: • Financial (42) • Public administration (39) • Media (25) • ICT (21) • Energy (18).
- The Institute noted a 150% increase of cyberattacks against entities in the Russian Federation despite a 25% decrease in the number of unique threat actors targeting Russian organizations. This increase in malicious cyber activities correlated with a slight increase in the activities of the IT Army of Ukraine, and the discovery of a new threat actor – Anonymous Italia. Furthermore, the increased targeting of Russian organizations correlated with a 285% increase in DDoS activities.
- The Institute also discovered a trend consisting of several cyber-enabled information operations directly impacting the citizens of the Russian Federation. Unknown pro-Ukrainian threat actor(s) conducted cyberattacks against Russian TV channels and radio stations and released false air alerts of missile strikes on the territory of the Russian Federation. The threat actor(s) was highly likely to be aiming to influence the Russian information space by increasing perceptions of proximity of Russian civilians to the conflict.

Other Countries

- 475 incidents against entities in other countries compared to 461 incidents documented throughout the whole of 2022. The majority of incidents recorded are DDoS attacks (95%).
- Top 3 targeted countries: • Poland (173) • Latvia (92) • United States of America (83).
- Top 3 targeted sectors: • Public administration (284) • Transportation (161) • Financial (93).
- The most active threat actors conducting attacks were the hacktivist collectives NoName057(16) (431), Anonymous Russia (100) and KillNet (88).
    - Notable threat actor activity: Anonymous Sudan (new threat actor).

3. Geopolitical Analyis

Russia has previously demonstrated its cyber capabilities by relentlessly attacking Ukraine's critical infrastructure and information space through campaigns[II] spanning several years. With this in mind, cyber and legal experts predicted a more destructive and visible cyber offensive further to the military invasion by Russia in February; however, this has not been the case. The Ukrainian network has proven to be more resilient. This Ukrainian resilience is partly due to the considerable amount of changes made since 2014 when Russia illegally annexed Crimea in regards to its own cybersecurity. Ukraine has also partnered with various countries and organizations such as the United States, NATO and the E.U. to help modernize their cybersecurity capabilities in order to protect itself.

4. Conclusion

At the Institute, Identifying and documenting cyberattacks is crucial. Whether they make the headlines or not, cyberattacks on the civilian population, and on infrastructure essential for its survival, cause differing degrees of harm, from undermining trust in institutions, disrupting core civilian and humanitarian services, spreading disinformation and preventing or impeding communication. The Institute will continue to document incidents in the context of the conflict and calls upon all actors to spare civilians and other protected persons, civilian objects and infrastructure which are ensuring the delivery of essential services in line with international humanitarian law. This is an obligation of all parties to the armed conflict. Respecting this law is important to save lives and reduce suffering.

II https://www.foreignaffairs.com/articles/russia-fsu/2022-01-28/how-russia-has-turned-ukraine-cyber-battlefield

References

1. This Policy Brief was prepared by the CyberPeace Institute, as part of T10.5.
2. The CyberPeace Institute has also published an article entitled "War in Ukraine: The struggle for computer network control and its impact on civilians". In this article, the Institute discusses how the war is not only taking place on the ground in Ukraine, but also across the internet, as well as the Russian Federation's willingness to impose borders within cyberspace in order to better control the flow of information. The article also goes into detail about the specificities of both the Russian and Ukrainian networks.
3. Cf. CyberPeace Institute (2022a), Cyber Dimensions of the Armed Conflict in Ukraine. Quarterly Analysis Report,Quarterly Analysis Report, Q3 July to September 2022, at: https://cyberpeaceinstitute.org/wp-content/uploads/Cyber%20Dimensions_Ukraine%20Q3%20Report.pdf.
4. Cf. CyberPeace Institute (2022b), Cyber Dimensions of the Armed Conflict in Ukraine. Quarterly Analysis Report,Quarterly Analysis Report, Q4 October to December 2022, at: https://cyberpeaceinstitute.org/wp-content/uploads/Cyber%20Dimensions_Ukraine%20Q4%20Report.pdf.
5. Cf. CyberPeace Institute (2023), Cyber Dimensions of the Armed Conflict in Ukraine. Quarterly Analysis Report, Q1 January to March 2023, at: https://cyberpeaceinstitute.org/wp-content/uploads/2023/05/Ukraine-Report-Q1_FINAL.pdf.