Research Report | XXXIV Annual Session

Special Conference 1

Countering the threat of Hybrid methods of warfare

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Student Officer name here

Forum	Special Conference 1
Issue:	Countering the threat of Hybrid methods of warfare
Student Officer:	Amelia Dorner
Position:	Deputy Chair

Introduction

In today's rapidly evolving world the nature of warfare has exceeded traditional boundaries leading to a more subtle and indirect form of warfare, called hybrid warfare. Initially introduced by US Marine Corps Lieutenant Colonel Frank G. Hoffman in 2006 as “complex irregular warfare” (Oxford Bibliographies), hybrid methods of warfare entail the use of military and non-military methods as a tool of subversion (NATO 2024). Namely, cyber attacks, political destabilization, disinformation campaigns, etc. To put simply, hybrid warfare is “the use of a range of different methods to attack an enemy, for example, the spreading of false information, or attacking important computer systems, as well as, or instead of, traditional military action” (Cambridge Dictionary). As specified by NATO, the aim of hybrid warfare is to damage an antagonistic state by destabilizing and undermining them. The use of hybrid warfare blurs the lines between war and peace and is recognized for its ambiguity and attribution. The issue of attribution is the difficulties that countries have in attributing certain actions to who actually did it. Hence, without an understanding of attribution it is difficult to retaliate and a collective response is weakened (Egmont Institute). Moreover, battle does not have a clear starting point making it challenging to effectively respond to such attacks at an appropriate time.

The most notable use of hybrid warfare was during Russia’s annexation of Crimea in 2014 . This event represents key characteristics of hybrid warfare and is consequently a defining example of hybrid warfare in the 21st century. The Russian Federation employed cyber attacks, disinformation campaigns, local proxy forces and their own unique tactics (Britannica). Since, the use of hybrid methods of warfare have become more prevalent and hence threatening to nations and alliances. Particularly affecting the North Atlantic Treaty Organization (NATO). NATO allies are facing threats from state and non-state actors who use hybrid warfare to target political institutions, influence public opinion, and undermine the security of NATO allies and their populations. Recently, the attacks have seen a change in speed, scale and intensity, becoming more threatening. To counter this, NATO

has developed a strategy for its role in countering hybrid warfare attacks and is prepared to defend its alliance and allies (NATO 2024).

Definition of Key Terms

Hybrid Warfare

Hybrid warfare is the employment of conventional and non-conventional means to exploit the vulnerabilities of a state while remaining below the threshold of formal warfare (NATO).

Cyber Attacks

A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device (IBM).

Disinformation campaigns

Disinformation campaigns are targeted and organised information attacks on companies, parties, institutions, or individuals in which false and misleading information is published with the intent to manipulate and deliberately disseminate false information (Prevency).

Economic pressure

Economic pressure is the strain and burden placed on the economy of a country due to factors such as scarcity of resources, unemployment rates, inflation, and debt levels.

Political destabilisation

Political destabilisation is the act of making a government, area, or political group lose power or control by causing changes and problems (Cambridge Dictionary).

Distributed Denial of Service (DDoS)

A distributed denial of service is the action of disrupting a normal functioning server by overwhelming it or its infrastructure with a flood of internet traffic. A website is only capable of receiving a certain amount of requests per minute and once that number exceeds the website performance diminishes (Check Point Software Technologies).

Ransomware Worms

Ransomware worms are malware that combine the characteristics of ransomware and worms to replicate itself and spread throughout a network. It encrypts and blocks a victim's personal data until a ransom (fee) is paid (Check Point Software technologies).

General Overview

Evolution of Hybrid Warfare

Hybrid warfare has evolved over time with new technological advancements. Since ancient and mediaeval times hybrid warfare has existed in various shapes and forms. For example, guerilla tactics and political manipulation and espionage. From there, religious propaganda and economic warfare were utilised during the Thirty Year War. In the World Wars, propaganda was prominent and in some instances guerilla tactics and sabotage were used. Later in the 20th century, there was more integration of psychological operations and propaganda, specifically in the Cold War. The development of the digital age introduced cyber warfare as a critical component of hybrid warfare. Today, hybrid warfare has become more prominent and threatening. The line between war and peace has become increasingly blurred calling for a solution from nations and alliances (NATO Foundation Defense College).

Components and Characteristics of Hybrid Warfare

Hybrid warfare is notable for its asymmetric qualities and increased emphasis on creativity, ambiguity, and the cognitive elements of war. Different instruments of power are used at different levels simultaneously creating a tailored attack to the vulnerabilities of an adversary (GOV.UK). Hybrid methods of warfare differ from humans' traditional understanding of warfare by intentionally exploiting ambiguity and creativity. In hybrid warfare, ambiguity is the ability to attack

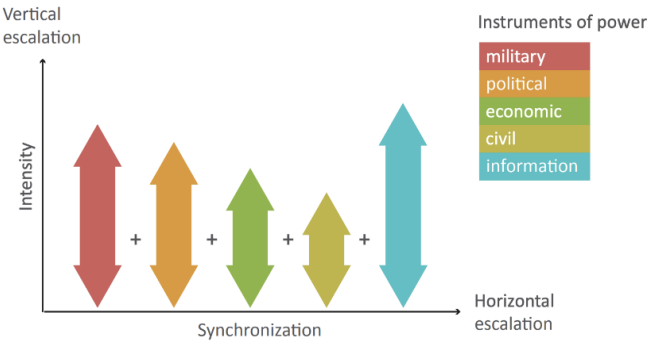

Figure 1: Graph showing variety of intensity and synchronization in Hybrid Warfare

an enemy with various synchronised elements, hence, forcing the enemy into a standstill as they are left confused by the attacks political, strategic and tactical intentions (Cambridge University Press). Furthermore, hybrid methods of warfare are capable of deliberately remaining under certain detection and response thresholds such as international legal thresholds due to the uncertainty and lack of visibility regarding the attack (GOV.UK). Consequently, the use of hybrid warfare hinders the decision process of the adversary in their counter attack because they are not aware of the attack. This makes hybrid methods of warfare more appealing to countries with the intention of attacking another country without retaliation, however, it also creates difficulties for nations and alliances such as NATO regarding their counterattack. Figure 1 shows an example of the variety of intensity and synchronisation that can be used in hybrid warfare to receive optimal results.

Significant examples of hybrid warfare attacks

Cyber attacks in Estonia

In the spring of 2007 Estonia was subject to a series of cyber attacks which lasted 22 days. The cause of the attacks was the political conflict between the Russian Federation and Estonia over the relocation of a Soviet-era monument in Tallinn. The cyber attacks began on the 27th of April 2007 and due to Estonia's small size and the immensity of the attacks it was seen as a threat to national security (CCDCOE). Furthermore, on many Russian forums and websites instructions on how to attack Estonian sites were distributed, an example of this is in Figure 2.


На 9-е МАЯ планируется повтор данной акции!
Не дай унизить своих соотечественников, отомсти за издевательства !!!
@ адреса eSStонских депутатов

Программа для рассылки писем
(пароль на RAR: nnm)

Нажми (пуск -> выполнить -> cmd)
введи ping -n 5000 -l 10000 эSStонский_сайт -t . и жми ENTER ВСЕ !!! Твои пламенные приветы полетели...
пример: ping -n 5000 -l 1000 www.riik.ee -t
Это 3 элементарных действия, после которых многие эстонские сайты просто перестанут работать!!!
Или вот .BAT файл, который в автоматическом режиме последовательно пингует эстонские DNS и MAIL сервера. Цикл бесконечен :)
Скопировать (красным) нижеприведённый текст, вставить в блокнот и сохранить как **priveteSStonia.BAT** (название можно любое) файл
(ты можешь сам добавлять адреса)

Figure 2: Cyber Attack Instructions found on Russian Forums on how to attack Estonia

Wannacry ransomware attack

Wannacry is a ransomware worm that spread throughout computer networks in May of 2017. According to Computer Security Online, Wannacry infiltrated thousands of computers across the world, exploited a vulnerability in Microsoft Windows operating system to encrypt users files and demanded a ransom in bitcoin (about $300) to regain access. The exploit known as EternalBlue tricks an unpatched version of Microsoft's implementation of the Server Message Block into executing arbitrary code. It is widely believed that the US discovered this vulnerability and rather than reporting it developed EternalBlue. However, this was stolen by a hacking group known as the Shadow Brokers and used to begin the Wannacry ransomware attack. It is also believed that the Lazarus Group with North Korean origin were behind this attack who have previously used DDoS attacks on South Korea and have hacked Sony and executed bank heists (CSO). The ransomware attack infected companies such as NHS, Telefonica, FedEx and even German Railway company Deutsche Bahn. Notably, the NHS was greatly affected as they had to shut down access to their networks to protect them. As a result, NHS England reported that the ambulance handover process and screens were disabled, CT/MR scans could not be transferred, Chemo orders were halted, transfers of blood results failed and GPs could not access their caseload (England NHS). Regardless that the objective of the Wannacry attack was likely for financial gain and not political gain, the feasibility of such a devastating cyber attack indicates the need for nations to develop defences against cyber attacks in the case that they are used in political conflicts such as the cyber attacks in Estonia.

Conflict between Russia and Ukraine

As the Russia-Ukraine war has evolved over the years, hybrid warfare has played a significant role in the Russian Federation’s strategies. The conflict originally began in 1991 when Ukraine gained independence from the Soviet Union. Since then, Ukraine has become a part of the European Union and NATO. Russia is particularly interested in Ukraine due to their strong familiar bonds going back centuries. Thus, after the Soviet Union collapsed, the loss of Ukraine was seen as a threat to Russia’s power.

In 1952 Crimea was transferred from Russia to Ukraine to strengthen the “brotherly ties between the Ukraine and Russian people''. However, after the fall of the Soviet Union Russian nationalists' sought to reclaim Crimea. In 2013/2014 tensions between Russia and Ukraine

heightened due to Ukraine's plans to strengthen its bond with the European Union. However, the Ukrainian president at the time Viktor Yanukovych decided to abandon the plans for economic integration with the EU sparking nationwide protests known as Euromaidan. These protests forced Yanukovych out of power allowing Russian President Putin to portray the protests as a Western-backed "fascists coup" which was a danger to the Russian population in Crimea hence commanding a covert military intervention in Crimea and justifying it as a humanitarian mission.

The annexation of Crimea is regarded as the first defining use of hybrid warfare. Initially, Russia began to regularly infuse Russian soldiers in Crimea posing as Ukrainian police. Hence, the invasion went unnoticed and it was over before the world could retaliate or comprehend what happened. Furthermore, disinformation and propaganda was heavily used. The Russian Government portrayed the Euromaidan protests as a fascist coup, framed the annexation as a humanitarian intervention to protect ethnic Russian citizens, and implemented false narratives by exaggerating the threats to Russian-speaking citizens of Western influences. Finally, the use of cyber attacks was crucial and led to the collapse of communication lines in Ukraine primarily between members of the parliament. Ukrainian government websites were also hacked and unavailable until 72 hours after the annexation of Crimea occurred. Considering this, the annexation was a clear example of hybrid warfare and how it contributed to the successful annexation of Crimea.

However, the tension between The Russian Federation and Ukraine continued to develop over the next 8 years up until the Russian invasion of Ukraine in February of 2022. Leading up to Russia's invasion in Ukraine on 24 February 2022 Russia was repeatedly cyber attacking Ukraine and intensified the cyber attacks right before the invasion. Over the period between the annexation of Crimea and the invasion of Ukraine, Ukraine's energy, media, public, businesses, and financial sectors suffered due to the cyber attacks. Following the invasion, cyber attacks also undermined the distribution of medicines, food and relief supply. Additionally, Russia employed disinformation leading up to the invasion, to justify its military actions and deny responsibility for their actions. One year after the beginning of the Russia-Ukraine war, in 2023, Russia's reputation was damaged and the nation was facing international sanctions. Hence, Russia turned to social media platforms to spread their propaganda on a global scale. Utilising fake social media networks, exploiting regional grievances against the West, hacking and forging documents, Russia spread a mix of old and

new narratives to undermine Ukraine and discredit it with Western allies and neighbouring countries hoping to diminish Ukraine's will to resist.

Major Parties Involved

Russian Federation

The Russian Federation is a dominant nation in the use of hybrid methods of warfare. It first used hybrid methods in several small wars during the 1990s and early 2000s. Specifically, during the Afghan War, Cechen Wars, Georgian War, Syrian War. Its use of hybrid warfare in the annexation of Crimea is also one of the first defining examples of the use of hybrid warfare for political and military purposes. Throughout its conflict with Ukraine Russia has implemented hybrid methods of warfare such as cyber attacks, disinformation campaigns and political destabilisation.

Ukraine

Ukraine has been the main target for Russian hybrid warfare attacks. Dealing with continuous cyber attacks and disinformation campaigns, Ukraine has had to adapt and improve its defence capabilities. The country has been a victim to countless cyber attacks targeting its infrastructure, government institutions and businesses. On top of this, Russia has attempted to weaken the country and diminish the support it is receiving through disinformation and propaganda. However, Ukraine has strengthened its ties with NATO and the EU and receives military, financial and technical support against the hybrid warfare attacks (NATO 2024).

China

China is another nation who has made use of hybrid warfare. Specifically in the South China Sea conflict, China employed hybrid warfare to assert its maritime jurisdictional rights and sovereignty. Specifically, they utilised espionage and economic leverage to influence regional actors. Moreover, China is also considered to conduct the most aggressive economic espionage in the world (Atlantic Council).

North Korea

North Korea's role in the hybrid method of warfare is its use of these tactics in notable attacks such as the Sony Pictures Hack in 2014 and the Wannacry ransomware attack in 2017 (CSO Online). It is suspected that the Lazarus Group was behind both of these attacks tying North Korea to them.

These events targeted crucial infrastructure throughout the world. Furthermore, North Korea utilises disinformation campaigns to manipulate international perceptions of the nation (ORB@binghamton.edu).

The North Atlantic Treaty Organization (NATO)

The North Atlantic Treaty Organization (NATO), established in 1949, is an alliance of 32 member states with the purpose of guaranteeing freedom and security for its members through military and political means. Recently, NATO has strengthened efforts to counter hybrid methods of warfare by improving allies' national resilience, promising to assist any allies against hybrid threats, set up counter-hybrid support teams, and endorsed preventive and response options to counter hybrid threats. Additionally, NATO has continued to strengthen its relationship with the European Union and collaborate with them on this matter by joining expertise and resources (NATO 2024).

European Union (EU)

Similar to NATO, the European Union has played a crucial war in countering hybrid warfare. Through their collaboration with other organisations such as NATO, creation and implementation of frameworks, and policy initiatives, the EU has developed comprehensive strategies to address hybrid threats. Initiatives such as the Hybrid Fusion Cell and the European Center of Excellence for Countering Hybrid Threats (Defence Industry and Space). Additionally, the EU works closely with NATO to leverage combined resources and expertise

Timeline of Key Events

Date	Description of event
February 19th, 1954	Russia Transfers Crimea to Ukraine
August 24th, 1991	Ukraine Gained Independence
February 20th, 2014	Crimea Annexation
November 24th, 2014	Sony Pictures Hack
April 11th, 2017	European Centre of Excellence for Countering Hybrid Threats Founded
May 12th, 2017	WannaCry Ransomware Attack

January 14th, 2022	Russia employs a Cyber Attack on Ukraine
February 24th, 2022	Russia invades Ukraine

UN involvement, Relevant Resolutions, Treaties and Events

Please do use either British or American spelling (and be consistent) throughout your Research Report. When listing past UN Resolutions, it is suggested that you make use of bullet points and the specified format below:

- Combating the criminal misuse of information technologies, 22 January 2001, (A/RES/55/63)
- Threats to international peace and security caused by terrorist acts, 27 January 2014, (S/RES/2133)
- Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, 17 March 2010, (A/RES/64/211)
- Budapest Convention on Cybercrime, 23 November 2001
- ATO Enhanced Forward Presence, 2016

Previous Attempts to solve the Issue

The Joint Framework on countering hybrid threats is a comprehensive approach with the aim of improving the response to the challenges posed by hybrid threats. It builds on the European Agenda on Security, EU Cyber Security Strategy, the Energy Security Strategy and the European Union Maritime Security Strategy. The Joint Framework combines existing policies and proposes 22 operational actions with the purpose of raising awareness, building resilience, preventing, responding and recovering to hybrid warfare using effective procedures, and increasing cooperation between the EU, NATO and other partner organisations (Commisiona Europa). While enhanced cooperation and raising awareness are more feasible to achieve, the effectiveness of the framework's aim to build resilience and use certain procedures against hybrid warfare has variability amongst member states. Due to the evolving nature of hybrid warfare the framework must be dynamic and flexible and requires updates and adaptations.

The European Center of Excellence for Countering Hybrid Threats, located in Helsinki, is a solution initiated in October 2017 by NATO Secretary General Jens Stoltenberg in collaboration with EU High Representative for Foreign Affairs and Vice-President of the European Commission Federica Mogherini. The centre's mission is to “strengthen its participating states and organisations security by providing expertise and training for countering hybrid threats” and it is open to all NATO and EU countries. The strong expertise and focus on education and training of the centre enhances the overall capability to understand and counter hybrid threats. However, there can be resource constraints as adequate funding is necessary for the centre to continue to operate and similar to the Joint Framework, the centre needs to be adaptable to the evolving nature of hybrid warfare.

Possible Solutions

A possible solution for countering the threats of hybrid methods of warfare is enhanced cyber defence and security. Cyber attacks are one of the main components of hybrid warfare and can heavily damage a country by posing financial and operational risks but also threatening a countries national security. Hence, enhanced cyber security is crucial and by reinforcing the capabilities of countries to prevent, detect and respond to cyber attacks, nations can help mitigate the impact of cyber attacks. This solution includes investing in cybersecurity technologies, enhancing resilience of infrastructure, and collaborating with other nations by sharing intelligence on cyber threats and response strategies.

Furthermore, strengthening legal and formative frameworks is another approach to addressing and countering hybrid warfare. The development and enforcement of clear legal frameworks help define prohibited actions and facilitate coordinated responses to hybrid threats. These frameworks could include measures to combat disinformation, regulate cyber attacks, and establish norms within the use of hybrid warfare. What is vital to consider in the creation of legal and formative frameworks is that they need to be adaptable to the evolution of hybrid warfare.

Finally, enhanced alliance cooperation can be crucial for effective countering of hybrid methods of warfare. Alliance cooperation enables members to leverage combined resources, expertise, and strategies. One of the weaknesses of the previous solutions is the risk of inadequate resources, however, if several member states are working together and providing resources the risk diminishes.

Overall, it is crucial to remember that hybrid warfare is dynamic due to its constantly changing nature as technology evolves and new threat actors are becoming involved (Hybrid CoE). Hence, all solutions need to take this into consideration and ensure that they are flexible and adaptable so that they can continue to be effective. One way to ensure this is to regularly monitor and evaluate the effectiveness of proposed solutions such as frameworks and initiatives to maintain their effectiveness and continuously improve them.

Bibliography

NATO - Homepage, https://www.nato.int/. Accessed 24 June 2024.

Alba, Kelcie. "North Koreans and the Fight Against Disinformation in Contemporary Society." *ORB@binghamton.edu*, https://orb.binghamton.edu/research_days_posters_2022/87/. Accessed 24 June 2024.

"Analysis of the 2007 Cyber Attacks against Estonia from the Inf." *CCDCOE*, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf. Accessed 24 June 2024.

Carvin, Andy, et al. "Undermining Ukraine: How Russia widened its global information war in 2023." *Atlantic Council*, 29 February 2024, https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/. Accessed 24 June 2024.

Cordesman, Anthony H., and Grace Hwang. "Chronology of Possible Russian Gray Area and Hybrid Warfare Operations." *CSIS*, 8 December 2020, https://www.csis.org/analysis/chronology-possible-russian-gray-area-and-hybrid-warfare-operations. Accessed 24 June 2024.

"DESTABILIZATION | English meaning - Cambridge Dictionary." *Cambridge Dictionary*, 17 July 2024, https://dictionary.cambridge.org/dictionary/english/destabilization. Accessed 21 July 2024.

"The Difference Between Ransomware and Malware - Check Point Software." *Check Point Software Technologies*,

https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/the-difference-between-ransomware-and-malware/. Accessed 21 July 2024.

"Fantastic portrait of a hacker. Cyber security internet concept. Generative AI." *Adobe Stock*, https://stock.adobe.com/images/fantastic-portrait-of-a-hacker-cyber-security-internet-concept-generative-ai/556157343.

"FAQ: Joint Framework on countering hybrid threats." *European Commission*, https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250. Accessed 21 July 2024.

"Frequently asked questions on hybrid threats." *Hybrid CoE*, https://www.hybridcoe.fi/wp-content/uploads/2024/01/FAQ-on-Hybrid-Threats.pdf. Accessed 21 July 2024.

Fruhlinger, Josh. "WannaCry explained: A perfect ransomware storm." *CSO Online*, 24 August 2022, https://www.csoonline.com/article/563017/wannacry-explained-a-perfect-ransomware-storm.html. Accessed 24 June 2024.

G.L.J., John, and WM Kitzen. "Hybrid Warfare - International Relations." *Oxford Bibliographies*, 22 September 2021, https://www.oxfordbibliographies.com/display/document/obo-9780199743292-0260.xml. Accessed 24 June 2024.

"Hybrid Threats - European Commission." *Defence Industry and Space*, https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en. Accessed 24 June 2024.

"Hybrid warfare: The continuation of ambiguity by other means." *Cambridge University Press*, Cambridge University Press,

https://www.cambridge.org/core/journals/european-journal-of-international-security/article/hybrid-warfare-the-continuation-of-ambiguity-by-other-means/1B3336D8109D418F89D732EB98B774E5.

Lewis, James A. "Is China's economic espionage the 'most aggressive' in the world?" *Atlantic Council*, 14 November 2012, https://www.atlanticcouncil.org/blogs/natosource/is-chinas-economic-espionage-the-most-aggressive-in-the-world/.

Marcuzzi, Stefano. "Hybrid Warfare in Historical Perspectives." *NATO Foundation Defense College*.

Masters, Jonathan. "Ukraine: Conflict at the Crossroads of Europe and Russia." *Council on Foreign Relations*, https://www.cfr.org/backgrounder/ukraine-conflict-crossroads-europe-and-russia. Accessed 24 June 2024.

"The NHS cyber attack: how and why it happened, and who did it." *Acronis*, 7 February 2020, https://www.acronis.com/en-eu/blog/posts/nhs-cyber-attack/. Accessed 24 June 2024.

"NHS England » NHS England business continuity management toolkit case study: WannaCry attack." *NHS England*, 21 April 2023, https://www.england.nhs.uk/long-read/case-study-wannacry-attack/. Accessed 21 July 2024.

Perry, William J. "How Russia's Hybrid Warfare is Changing." *Small Wars Journal*, 17 July 2023, https://smallwarsjournal.com/jrnl/art/how-russias-hybrid-warfare-changing. Accessed 24 June 2024.

Przetacznik, Jakub, and Simona Tarpova. “Russia's war on Ukraine: Timeline of cyber-attacks.” *European Parliament*, 8 June 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf. Accessed 24 June 2024.

“Russia's hybrid warfare strategy: From Crimea to Ukraine.” *Observer Research Foundation*, 1 March 2022, https://www.orfonline.org/expert-speak/russias-hybrid-warfare-strategy. Accessed 24 June 2024.

Siman, Bernard. “Hybrid Warfare: Attribution is Key to Deterrence.” *Egmont Institute*, 30 January 2023, https://www.egmontinstitute.be/hybrid-warfare-attribution-is-key-to-deterrence/. Accessed 21 July 2024.

Stebelsky, Ihor. “Ukraine - Crimea, Eastern Ukraine, Conflict.” *Britannica*, https://www.britannica.com/place/Ukraine/The-crisis-in-Crimea-and-eastern-Ukraine. Accessed 24 June 2024.

“Understanding Hybrid Warfare.” *GOV.UK*, https://assets.publishing.service.gov.uk/media/5a8228a540f0b62305b92caa/dar_mcdc_hybrid_warfare.pdf. Accessed 24 June 2024.

“What is a Cyberattack?” *IBM*, https://www.ibm.com/topics/cyber-attack. Accessed 24 June 2024.

“What is a disinformation campaign? - PREVENCY®.” *prevency*, https://prevency.com/en/what-is-a-disinformation-campaign/. Accessed 24 June 2024.

“What is DDoS Attack? - Types of DDoS Attacks - Check Point Software.” *Check Point Software Technologies*,

https://www.checkpoint.com/cyber-hub/cyber-security/what-is-ddos/.

Accessed 24 June 2024.

"What is Hybrid CoE?" *Hybrid CoE*, https://www.hybridcoe.fi/who-what-and-how/.

Accessed 24 June 2024.