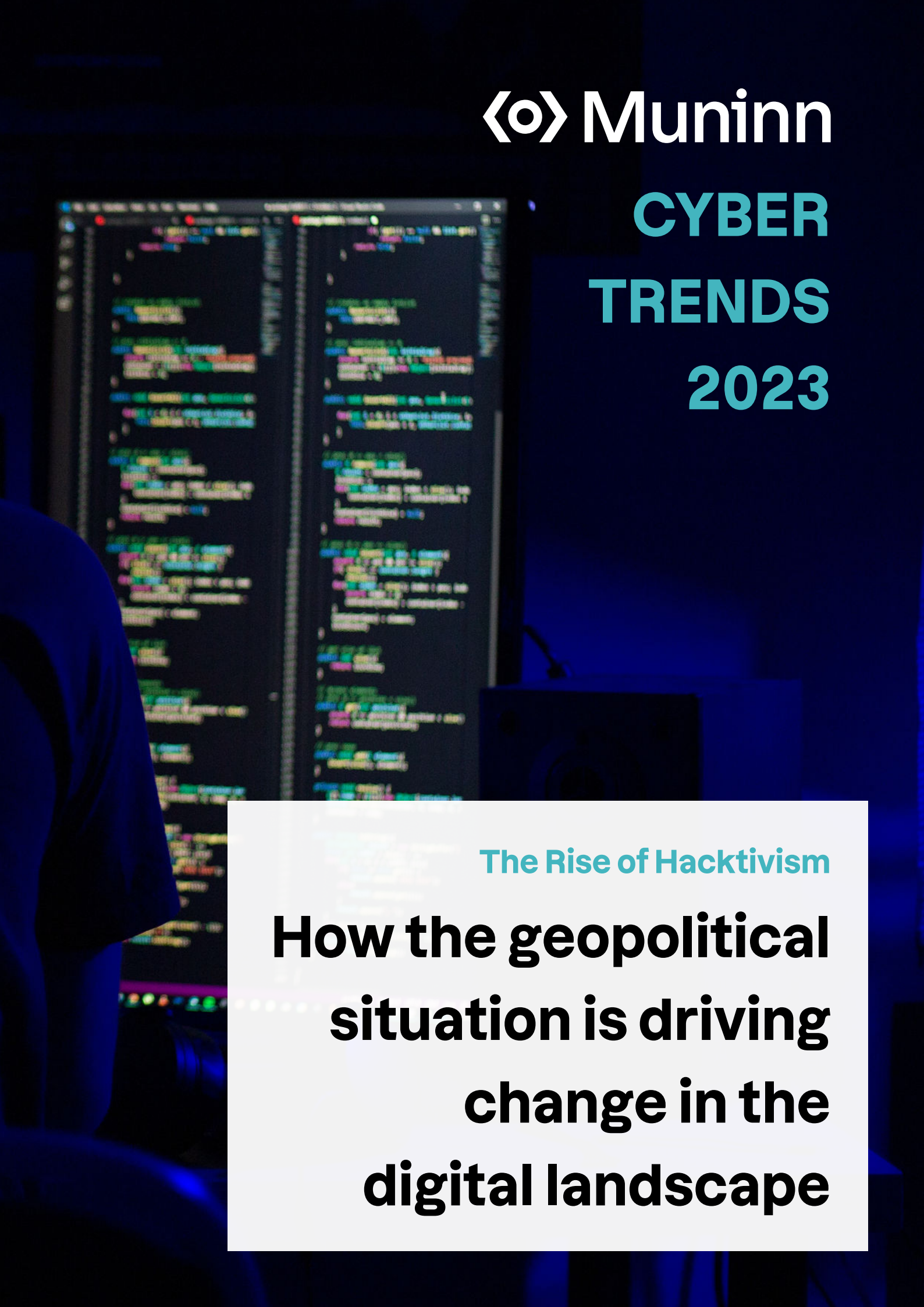
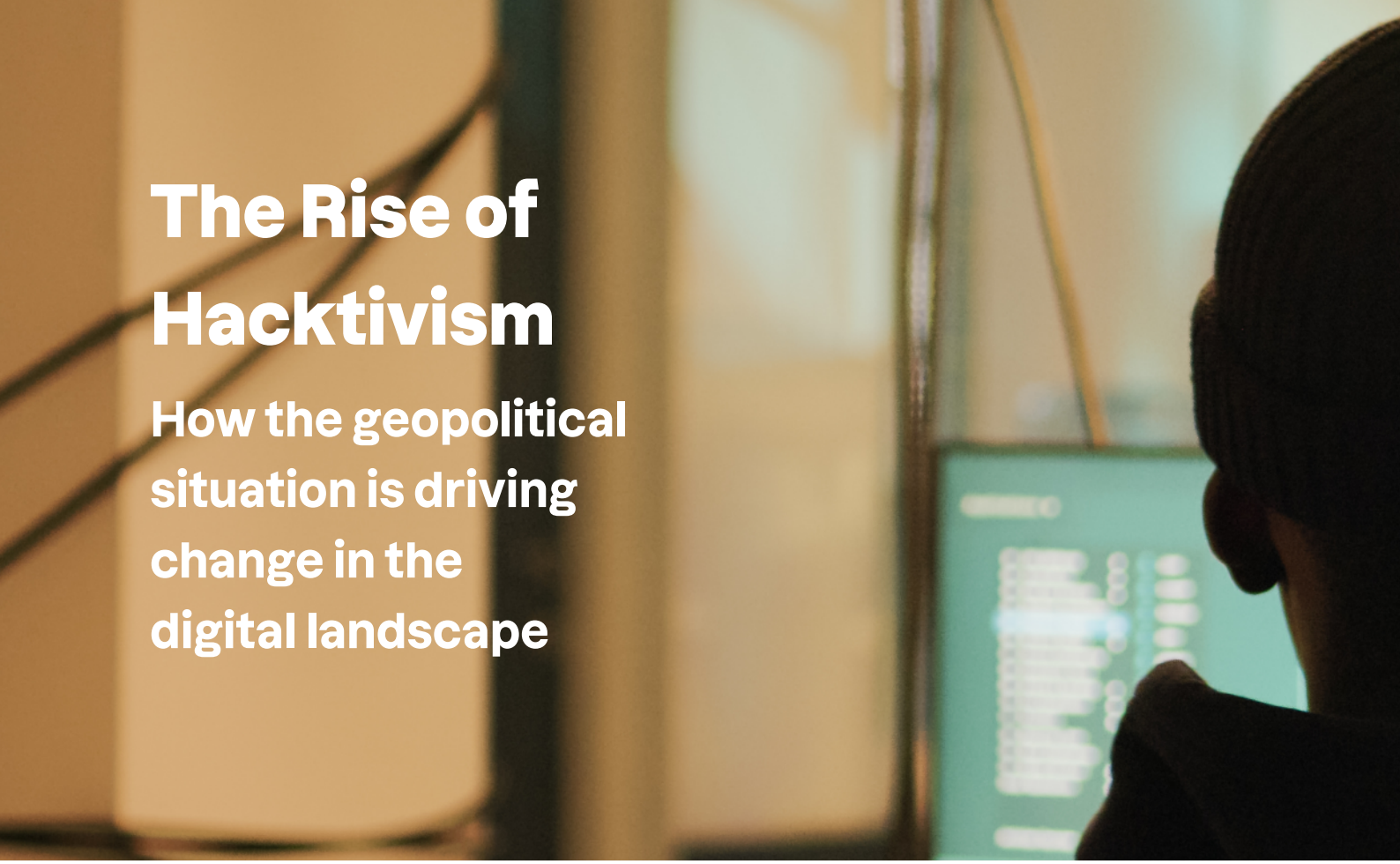


Muninn

CYBER TRENDS 2023

The Rise of Hacktivism

How the geopolitical situation is driving change in the digital landscape



The Rise of Hacktivism

How the geopolitical situation is driving change in the digital landscape

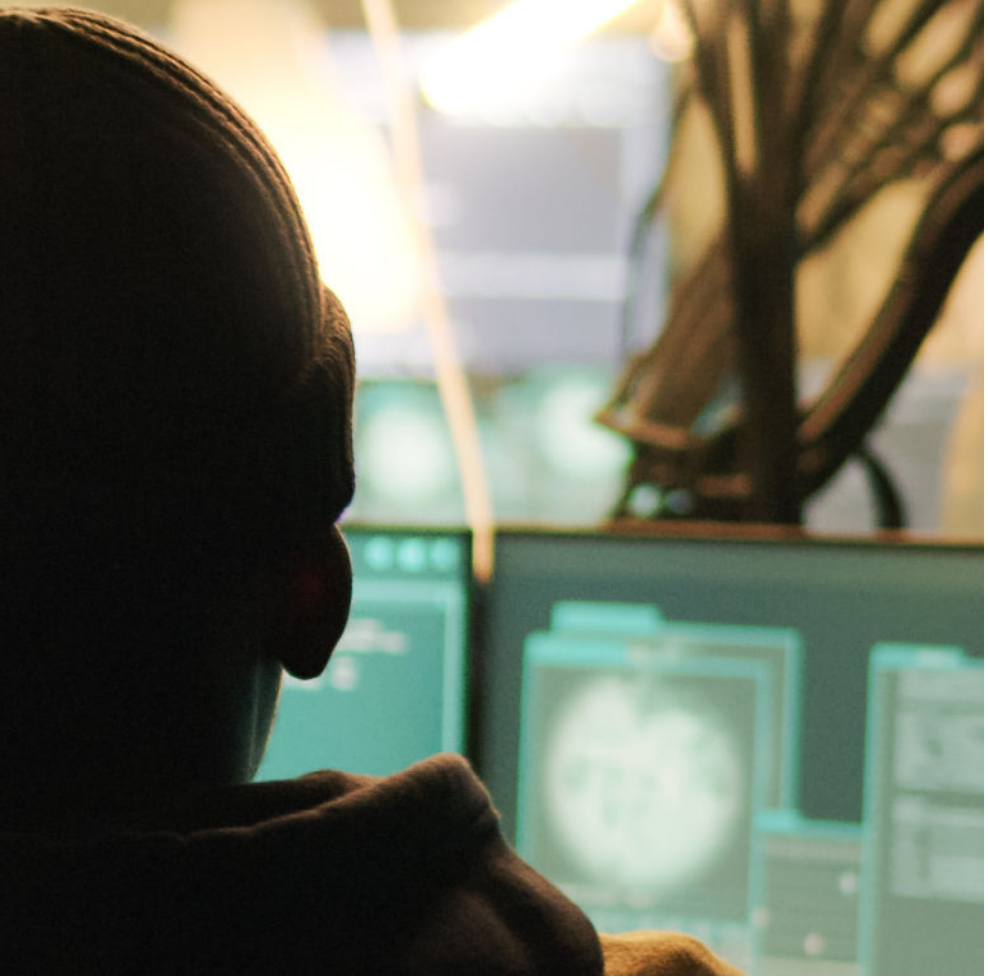
In recent years, hacktivism has undergone a significant transformation. The once disorganized and fluid social groups like Anonymous were known for their diverse agendas and lack of long-term strategy. From taking on hate groups to pilfering government secrets, hacktivist campaigns have been making waves for years. Some of the more notable old-school examples include Operation KKK, a direct attack against Ku Klux Klan members and supporters, and Operation AntiSec, which sought to obtain and leak classified government documents. But a new breed of hacktivist groups has entered the digital stage. These new groups are more focused, structured, and sophisticated, and their operations have become a growing concern for governments and corporations worldwide.

Known as "Hacktivism 2.0," this new era of hacktivism has arisen in response to conflicts in Eastern Europe and the Middle East. These state-mobilized hacktivist groups are responsible for carrying out major cyber attacks against governments and corporations across the West. The impact of these attacks has been significant, with countries like the United States, Germany, Lithuania, Italy, Estonia, Norway, Finland, Poland, and Japan being particularly targeted.

The new hacktivist groups operate like structured organizations, characterized by a clear political ideology, a hierarchy for their members and leaders, and even a formalized recruitment process. They have a strong public relations presence, carefully crafting and publicizing their success stories to highlight their significant impact in the cyber world.

Their operations are no longer limited to petty distributed denial of service (DDoS) or defacement attacks on low-profile websites. Instead, they are capable of carrying out large-scale, disruptive attacks against their targets such as government agencies and organizations, often with an extensive public relations campaign to magnify their impact, becoming a significant threat that these groups pose to both private and public entities.

> Anonymous first became associated with hacktivism in 2008 after carrying out a series of actions against the Church of Scientology called Project Chanology. The Church responded with a cease-and-desist letter to a video of Tom Cruise praising the religion. In retaliation, 4chan users organized a raid against the Church, involving prank-calling its hotline, sending black faxes to waste ink cartridges, and launching DDoS attacks on Scientology's websites.



> NoName057(16) is among the pro-Russian groups performing DDoS attacks on websites belonging to governments, news agencies, suppliers, telecommunications companies, and more in Ukraine and neighboring countries supporting Ukraine.

Hacktivism 2.0 and the shift to Government Agendas

Two years ago, a shift in hacktivism began to emerge in the Middle East. Several hacktivist groups like Hackers of Savior, Black Shadow, and Moses Staff quietly rose to prominence, focusing solely on launching attacks against Israel. These groups did not shy away from their affiliation with the Iranian regime's anti-Israel narrative. At the same time, other groups in the region dedicated themselves to targeting pro-Iranian entities, united only by their opposition to the Iranian regime.

However, this phenomenon isn't exclusive to the Middle East. The ongoing Russian-Ukrainian war has also been shaped by hacktivism. In early 2022, the Belarusian Cyber-Partisans, a group established in 2020 to oppose the Belarussian government, began launching devastating cyberattacks to obstruct Russia's troops.

The hacktivist group that has been most vocal in its support of Ukraine is TeamOneFist, a pro-Ukraine collective that caused a blackout at the airport in Khanty-Mansiysk City, Russia, after targeting the natural gas power plant in August last year.

With the rise of hacktivism, the Ukrainian government has mobilized the IT Army of Ukraine to launch a series of cyberattacks against Russia. This new wave of hacktivism has also given rise to groups that support the Russian geopolitical narrative, including Killnet, Xaknet, From Russia with Love (FRwL), and NoName057(16), among others.

The Russian-mobilized groups initially focused on specific geographical areas but have since expanded their scope to target anyone opposing the Russian agenda, from Europe and the United States to Asia. These attacks have included significant assaults on the governments and major corporations of various countries, including the US, Lithuania, Italy, Estonia, Norway, Finland, Poland, Japan, and more. One notable example is NoName057(16)'s cyberattack on the website of the Finnish Parliament in August 2022 after Finland expressed interest in joining NATO.

KillNet

The new kids on the block

The group's expanded focus resulted in a significant increase in the range of targets, including high-profile ones like major government websites, airports, and more. While the impact of some of these attacks is difficult to gauge, many of them have proven to be successful. They have caused significant downtime for major websites, some of which provide essential public services.

The group's attacks have targeted a wide range of high-profile targets, including major government websites and airports, among others. While the full extent of the damage caused by these attacks is difficult to determine, many of them have resulted in some downtime for major websites that provide essential public services. However, most countries on the receiving end of Killnet's attacks have been able to fend off the attacks or easily recover from them.

But Killnet's reputation stems not from its hacking capabilities or advanced methods, but more from its ability to disrupt services and claim victory in grandiose ways. The group is known for its flamboyant PR tactics, including flashy announcement videos, memes, and watermark images, which are shared on social media and reported by news outlets. While Killnet has expressed interest in collaborating with the Russian government, there is currently no evidence that it is under state control.

How they organize

Hacktivist groups are gaining traction in the cyber world, with an increasing number of followers joining their cause. Bound by a shared manifesto and clear rules, these groups represent a new frontier in cyber warfare. With over 89,000 subscribers on their Telegram channel, Killnet is one of the most prominent groups, being highly organized, boasting a military-like structure with a top-down hierarchy and multiple specialized squads responsible for executing their missions.

At the heart of Killnet's operations is its former leader, KillMilk. The group employs a decentralized approach, with each small squad having its own designated commander, improving the group's overall survivability. This tactic has proven highly effective as the group continues to grow in size and power. Killnet's rules and targets are laid out on their Telegram page, along with instructions on how to join or create additional squads for those seeking more autonomy or advancement within the group.

This strategy has allowed Killnet to recruit new members at an impressive rate, further bolstering their capabilities.

Killnet's success has not gone unnoticed, and other groups are now seeking to collaborate or even join forces altogether. As the group continues to evolve, it remains to be seen how far they will go and what impact they will have on the world of cyber warfare. With their strategic organization, clear structure and growing ranks, Killnet is a force to be reckoned with.

Killnet activities world-wide

Norway – In a coordinated effort, Killnet hackers launched a series of DDoS attacks against Norwegian organizations on June 28, 2022. The targets of the attacks and the extent of the damage caused remain unclear. However, the National Security Authority of Norway released a statement confirming that no private data was compromised during the attacks. .

Italy – In May 2022, Killnet launched a highly publicized attack on the Eurovision song contest. Russia was prohibited from competing in the competition, so the hacking group attempted to carry out a DDoS attack. The attack was ultimately blocked by Italy's police department, but the country didn't escape unscathed. Killnet retaliated by hitting the Senate and National Health Institute websites with similar attacks. Despite being thwarted, the attack demonstrated the group's boldness and their willingness to take on high-profile targets.

USA – The group's actions have included a distributed denial of service (DDoS) attack on Bradley International Airport in Connecticut, which was confirmed by US authorities in March of 2022.

Killnet has also claimed responsibility for a cyberattack on Lockheed Martin, a major US defence corporation. The attack was carried out in retaliation for the US supplying HIMARS systems to Ukraine, which Killnet sees as an act of aggression against Russia. The group's founder, known as "Killmilk," has accused Lockheed Martin of sponsoring "world terrorism" and being responsible for "thousands and thousands of human deaths." Killmilk announced prior to the attack that it would be a new type of cyberattack targeting the company's production systems as well as information about its employees.

Japan –The group targeted several high-profile Japanese websites in September, in response to Japan's support for Ukraine in the escalating Russian-Japanese conflict over the Kuril Islands.

Killnet's attacks were highly effective and caused significant disruptions to key Japanese websites. The group successfully targeted the e-government website, the public transportation websites for Tokyo and Osaka, the JCB payment system, and Mixi, which is Japan's second largest social media site.

Germany: German government and politicians' websites have been targeted by Killnet, as well as those of other high-profile organizations. The attacks were in response to the German government's decision to supply military equipment to Ukraine.

January 26th 2023 the German Federal Office for Information Security (BSI) announced a wide-ranging DDoS attack against various agencies and companies in Germany. Airports, companies in the financial sector, and federal as well as state administrations were particularly affected. Killnet had reportedly announced the attacks in advance as retaliation for Germany's decision to send Leopard 2 battle tanks to Ukraine.

Finding new talent

Once opening their doors for everyone interested, Hacktivist groups now are taking a more exclusive approach to recruitment, seeking out only the most skilled and knowledgeable hackers or experts in specific fields to join their ranks. This approach is aimed at minimizing the risk of mistakes that could expose the group's entire operation. By handpicking the most capable members, these groups hope to build a team that can operate with precision and efficiency. However, some groups are struggling to find enough skilled hackers, leading to a recent trend of relaying DDoS attack instructions to the masses and enlisting the help of a wider pool of less-skilled individuals to carry out their attacks.

New World Order

The past few years have been marked by an upswing in conflict across Eastern Europe and the Middle East, with far-reaching consequences for people's lives and geopolitical situations around the globe. One of the most striking effects of these conflicts has been the escalation of tensions in the world of cyberspace.

Where once the term "hacktivism" was little more than a buzzword, today it represents a serious and growing threat to global organizations. Hacktivist groups have become increasingly organized, structured, and sophisticated, ushering in a renaissance era for this type of activity. Of particular concern is the fact that many of these groups have clear affiliations with specific states, serving the interests of those governments at the expense of other countries and organizations.

While hacktivism initially emerged as a phenomenon associated with specific conflict areas, it has rapidly spread to other parts of the world. This proliferation is expected to continue, with hacktivist operators enhancing their arsenals and unleashing increasingly sophisticated and damaging state-level attacks. What's more, an increasing number of governments are taking note of the success of state-mobilized hacktivist groups and may seek to create their own, making it clear that this phenomenon is here to stay.

Whether you view hacktivism as a legitimate form of dissent or a dangerous threat to cybersecurity, it is impossible to deny the profound impact it has had on politics and activism. By blurring the line between virtual and real-world activism, hacktivism has forced society to re-evaluate what it means to engage in dissent and activism in the digital age, and to confront the new and often unpredictable challenges of this new era.

References:

https://en.wikipedia.org/wiki/Anonymous_(hacker_group)

https://www.wired.co.uk/article/hacktivism-russia-ukraine-ddos

https://thecyberexpress.com/the-scariest-ransomware-groups-in-2023/

https://www.helpnetsecurity.com/2023/01/18/cybersecurity-in-2023-russian-escalation-chinese-espionage-iranian-hacktivism/

https://www.bloomberg.com/news/articles/2022-06-30/russian-hackers-target-norway-in-latest-volley-of-cyber-attacks

https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/

https://en.wikipedia.org/wiki/Killnet#cite_note-14

https://www.bleepingcomputer.com/news/security/us-airports-sites-taken-down-in-ddos-attacks-by-pro-russian-hackers/

https://www.darkreading.com/ics-ot/killnet-pro-russia-hacktivist-group-support-influence-grows

https://www.computerweekly.com/news/365530999/Killnet-DDoS-attacks-disrupt-Nato-websites

https://www.jpost.com/israel-news/moses-staff-hackers-strike-again-attack-israeli-engineering-companies-683855