NORWICH UNIVERSITY

2024 Richard S. Schultz '60 Symposium Fellow Research Report

How Anonymous Sudan Leverages Perception in its Cyber Operations Against Israel

A THREAT PROFILE

By: Lucia Frezza, Schultz Fellow

Advised by: Mark Perry, Lead Research Analyst - Information Warfare

Advised by: John Kidder, Information Warfare Subject Matter Expert

Contents

NORWICH™
UNIVERSITY

Abstract

Cyber threat actors utilize influence operations and social media to gather support for their operations. With the rise of technology, this intersection between cyber operations and influence operations is a growing part of conflict. Independent cyber threat actor, *Anonymous Sudan* weaponizes outside perception on cyber operations to generate influence. Leveraging Telegram, social media and cyber operations, *Anonymous Sudan*, controls perception of their actions to grow awareness for their pro-Palestinian viewpoint and to conduct cyber operations against Israel as an independent cyber threat actor.

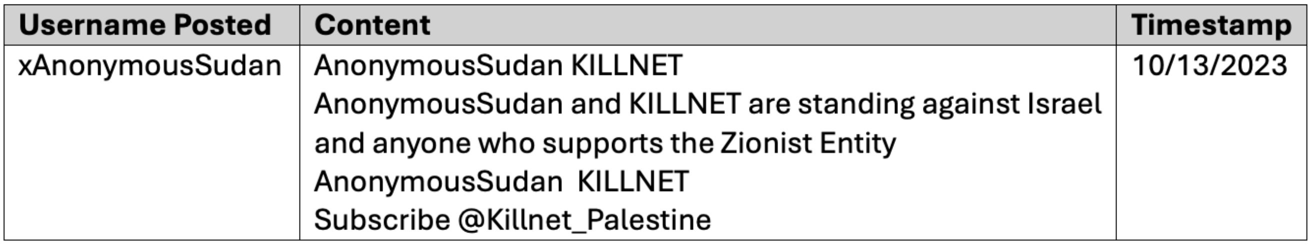
Introduction

Increasingly, the perception of cyberwarfare is being used by independent threat actors as a form of influence. While controlling perception is not new in warfare, globalization and the rise of technology makes this intersection between influence and cyberwarfare more critical to understand for the future of warfare. (Thomas, Thompson, & Wanless, 2020). The perception of cyberwarfare significantly influences modern conflict, which now encompasses the art of influencing someone's actions, behaviors, and beliefs. Influence itself is hard to quantify, but one can measure cyberattacks, posts, and sentiments to see a possible change in perception of audiences or how they were influenced. Hence, the technological world is seeing more need to control its perception, especially in areas of conflict.

Cyber conflict includes the more common malicious activities such as hacking – stealing, destroying or disrupting data on the internet. However, within conflict, cyber conflicts are more for the disruption, destruction, and theft of data to achieve a goal within the greater conflict. Cyber threat actors in conflicts use their tools, skills, and software to support their side in the conflict. Historically, these activities were kept out of the public eye, but more recently both state-based and independent threat actors are more overt in these actions. This affects how their operations are done and how much support they receive. Independent cyber threat actors weaponize perception and leverage social media in order to strengthen their cause. In this article, the threat profile of Anonymous Sudan will be analyzed based on the groups' Telegram activity and correlating cyber activity connected to the conflict in Gaza. Classified as a 'hacktivist' group, Anonymous Sudan identifies targets around the world to not only conduct cyber operations against, but also to influence for or against a cause. (Anonymous Sudan, n.d.).

Anonymous Sudan: An Introduction

Anonymous Sudan, otherwise known as Storm-1359, is an independent cyber threat actor whose overall cause is to attract attention and draw focus to the tragic situation in Sudan. (Perry, 2024). *Anonymous Sudan* is a classic example of a hacktivist, or a group that will hack, destroy, steal, or disrupt data to bring attention to their causes. As an independent threat actor, meaning they aren't known in direct connection to a government, they are able to be involved with several conflicts and situations at once. For example, they have worked in conjunction with other hacktivist groups such as Killnet, a Russian cyber threat actor who has been involved with several conflicts and situations globally (Operator, 2024). Following the lead of their Russian counterparts in Killnet, they are currently active in the Israel-Hamas conflict (KillNet Group, n.d.).

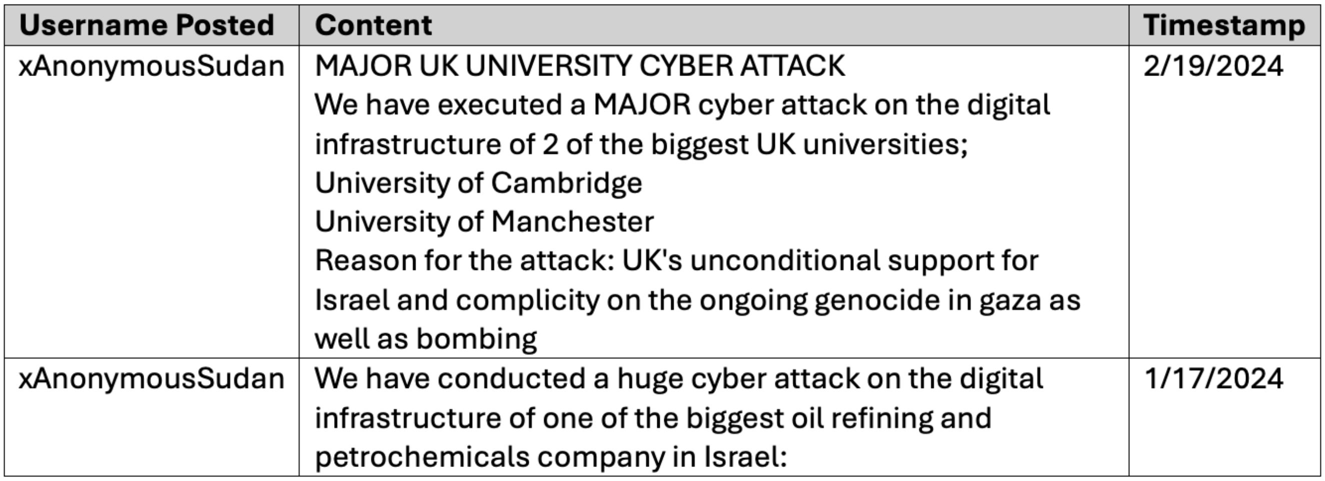


Username Posted	Content	Timestamp
xAnonymousSudan	AnonymousSudan KILLNET AnonymousSudan and KILLNET are standing against Israel and anyone who supports the Zionist Entity AnonymousSudan KILLNET Subscribe @Killnet_Palestine	10/13/2023

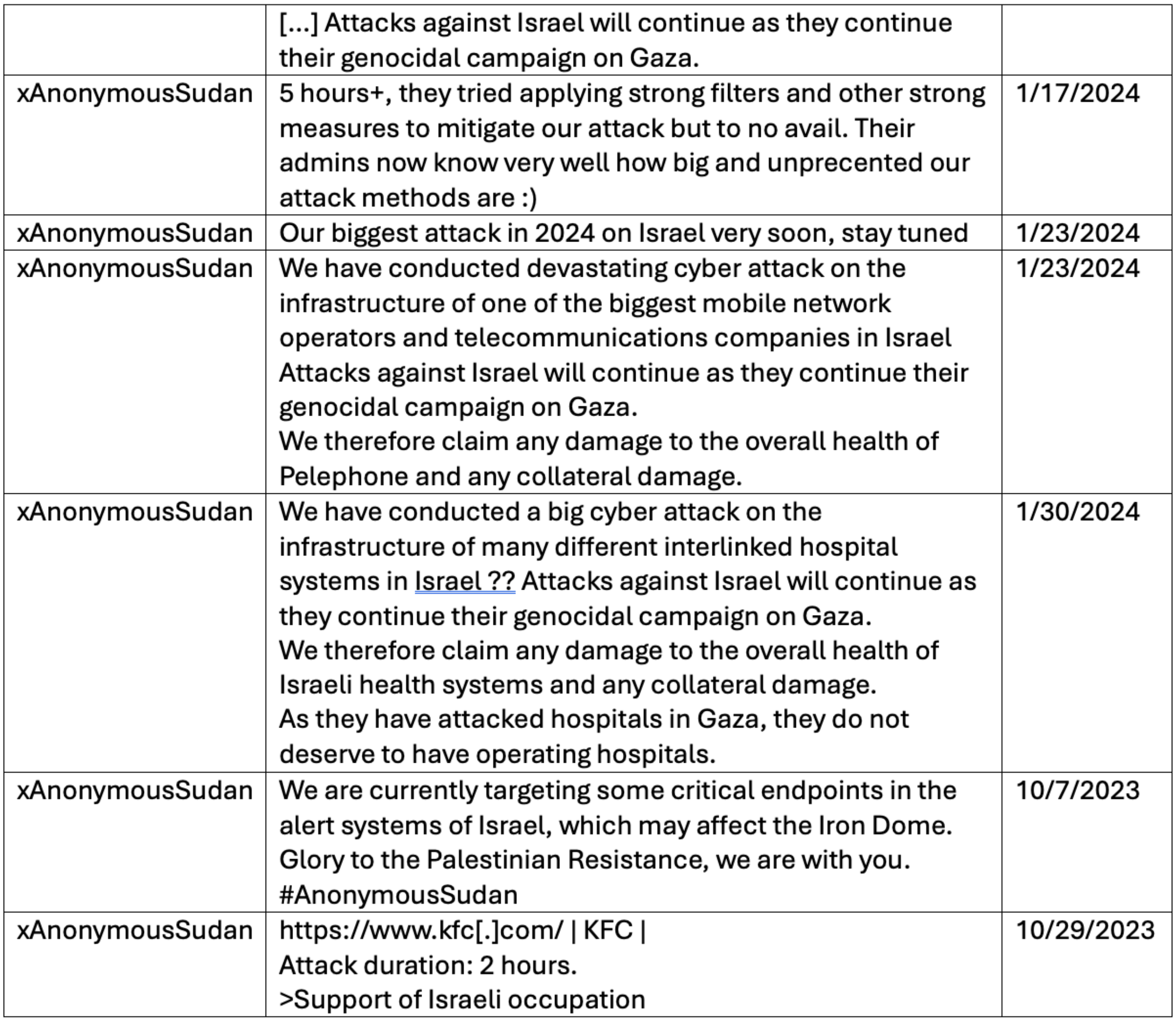
Figure 1. message archive sample Anonymous Sudan and Killnet support (Perry, 2024)

They are very active in this conflict, posting their attacks and updates, advertising for their services and posting news articles detailing their exploits on their social media account, xAnonymousSudan, on Telegram. As a hacktivist group, they use their attacks and products to support causes either through directly attacking those for the cause they are against, or to bring awareness of a cause to a greater audience and influence them to agree.

Anonymous Sudan targets a large variety of companies, countries, and sectors in order to bring the widest audience into their fold. Like other hacktivists, they often target sectors such as telecommunications, health, academia, and other nongovernmental industries. Some of their targets and campaigns are shown in the figure below that was taken from their Telegram channel in the form of a message archive.



Username Posted	Content	Timestamp
xAnonymousSudan	MAJOR UK UNIVERSITY CYBER ATTACK We have executed a MAJOR cyber attack on the digital infrastructure of 2 of the biggest UK universities; University of Cambridge University of Manchester Reason for the attack: UK's unconditional support for Israel and complicity on the ongoing genocide in gaza as well as bombing	2/19/2024
xAnonymousSudan	We have conducted a huge cyber attack on the digital infrastructure of one of the biggest oil refining and petrochemicals company in Israel:	1/17/2024

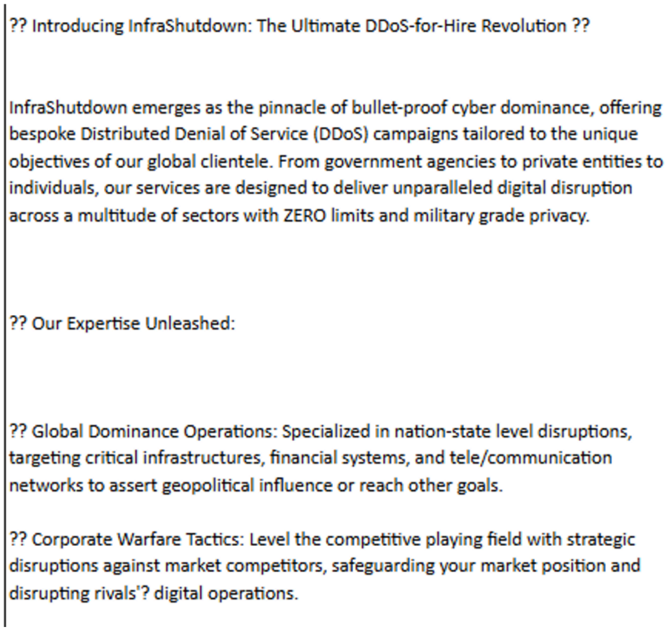


	[…] Attacks against Israel will continue as they continue their genocidal campaign on Gaza.	
xAnonymousSudan	5 hours+, they tried applying strong filters and other strong measures to mitigate our attack but to no avail. Their admins now know very well how big and unprecented our attack methods are :)	1/17/2024
xAnonymousSudan	Our biggest attack in 2024 on Israel very soon, stay tuned	1/23/2024
xAnonymousSudan	We have conducted devastating cyber attack on the infrastructure of one of the biggest mobile network operators and telecommunications companies in Israel Attacks against Israel will continue as they continue their genocidal campaign on Gaza. We therefore claim any damage to the overall health of Pelephone and any collateral damage.	1/23/2024
xAnonymousSudan	We have conducted a big cyber attack on the infrastructure of many different interlinked hospital systems in Israel ?? Attacks against Israel will continue as they continue their genocidal campaign on Gaza. We therefore claim any damage to the overall health of Israeli health systems and any collateral damage. As they have attacked hospitals in Gaza, they do not deserve to have operating hospitals.	1/30/2024
xAnonymousSudan	We are currently targeting some critical endpoints in the alert systems of Israel, which may affect the Iron Dome. Glory to the Palestinian Resistance, we are with you. #AnonymousSudan	10/7/2023
xAnonymousSudan	https://www.kfc[.]com/ | KFC | Attack duration: 2 hours. >Support of Israeli occupation	10/29/2023

Figure 2. message archive sample illustrating Anonymous Sudan threats to Israel (Perry, 2024)

Threats, warnings, and claims of victory are common; Figure 2 shows a sample from a message archive scrapped directly from Telegram where *Anonymous Sudan* demonstrates their support of pro-Palestinian ideals. *Anonymous Sudan* amplifies their own narrative about the war. This has the aim to emotionally affect readers. They target companies and organizations that have shown support to Israel or Israel's causes. The examples shown above are from October 2023 to early 2024. This shows only a concentrated portion of their attacks and timeline. It should be noted that while *Anonymous Sudan* is very active in this crisis, they also have their own personal motivations and targets outside of the conflict. These include political targets, pro-Sudanese and pro-Russian, targets motivated by religion, pro-Islamic, and financial gain, by extortion and DDOS (Operator, 2024). They have many too many causes and are heavily related to Killnet, even being "inaugurated" by the Russian cluster (Operator, 2024). This means that their goals and objectives are going to match those of their Russian counterparts, and that they will be bolder in bigger conflicts with this backing.

Anonymous Sudan is characterized for their botnet and DDOS attack capabilities, both of which they have promoted and sold to exclusives through their social media followings. Denial-of-Service attack, or DOS, uses overwhelming network traffic to overwhelm victim servers and infrastructure to halt operations.



?? Introducing InfraShutdown: The Ultimate DDoS-for-Hire Revolution ??

InfraShutdown emerges as the pinnacle of bullet-proof cyber dominance, offering bespoke Distributed Denial of Service (DDoS) campaigns tailored to the unique objectives of our global clientele. From government agencies to private entities to individuals, our services are designed to deliver unparalleled digital disruption across a multitude of sectors with ZERO limits and military grade privacy.

?? Our Expertise Unleashed:

?? Global Dominance Operations: Specialized in nation-state level disruptions, targeting critical infrastructures, financial systems, and tele/communication networks to assert geopolitical influence or reach other goals.

?? Corporate Warfare Tactics: Level the competitive playing field with strategic disruptions against market competitors, safeguarding your market position and disrupting rivals'? digital operations.

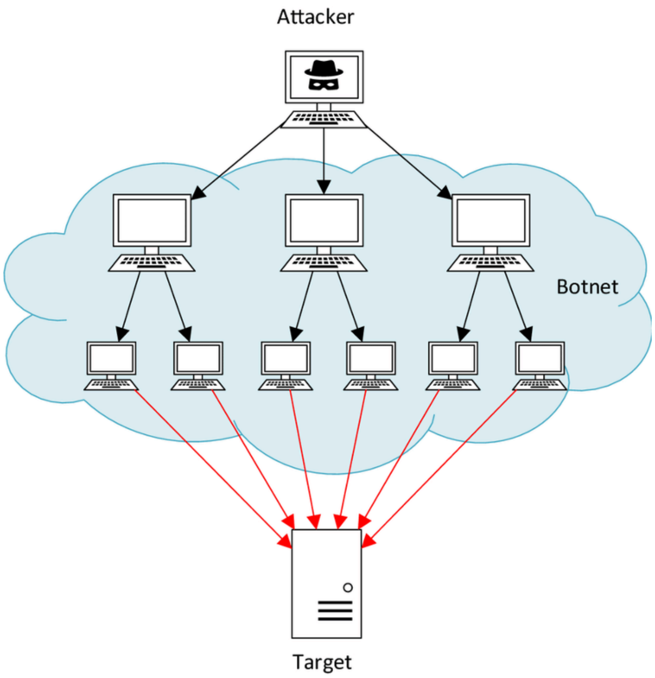
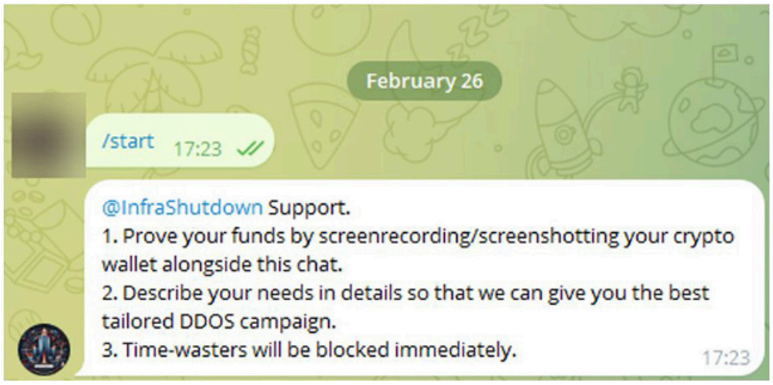


Figure 3(left). Anonymous Sudan's advertising post for InfraShutdown (Perry, 2024)

Figure 4(right). Example of a botnet used for a DOS attack (Najafimehr, 2022)

Anonymous Sudan often uses commercial products such as Skynet botnet families and Godzilla, a very popular botnet. For their Israeli campaign they partnered with a new infrastructure attack product, InfraShutdown. Advertising for this product is done via their main Telegram channel and direct messaging. InfraShutdown and Anonymous Sudan request proof of funds and a need for their DDOS services. This is to create a more exclusive offering.



February 26

/start 17:23

@InfraShutdown Support.
1. Prove your funds by screenrecording/screenshotting your crypto wallet alongside this chat.
2. Describe your needs in details so that we can give you the best tailored DDOS campaign.
3. Time-wasters will be blocked immediately.
17:23

Figure 5. Anonymous Sudan Chat showing request for proof (Operator, 2024)

Anonymous Sudan's targets vary, and they have targeted several countries and companies in connection to their Israeli campaign. Most notably, they targeted ChatGPT and Cloudflare, ChatGPT's cybersecurity provider. High-profile targets like these can help their reputation and that of the services they provide. They also targeted several industries specifically within Israel such as oil, telecommunications, academia, and news outlets.

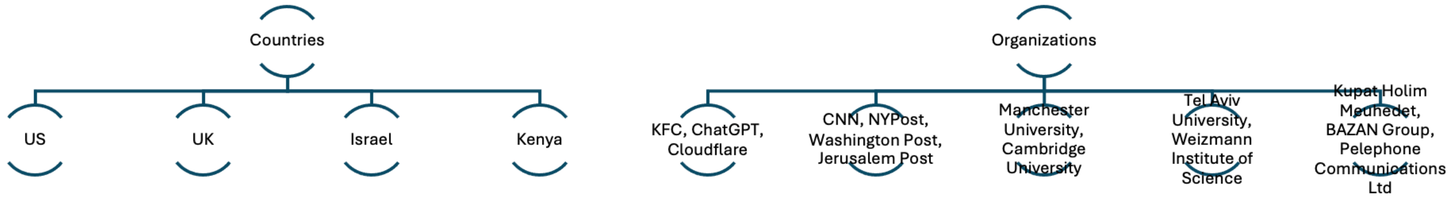

Countries
US
UK
Israel
Kenya
Organizations
KFC, ChatGPT, Cloudflare
CNN, NYPost, Washington Post, Jerusalem Post
Manchester University, Cambridge University
Tel Aviv University, Weizmann Institute of Science
Kupat Holim Meuhedet, BAZAN Group, Pelephone Communications Ltd

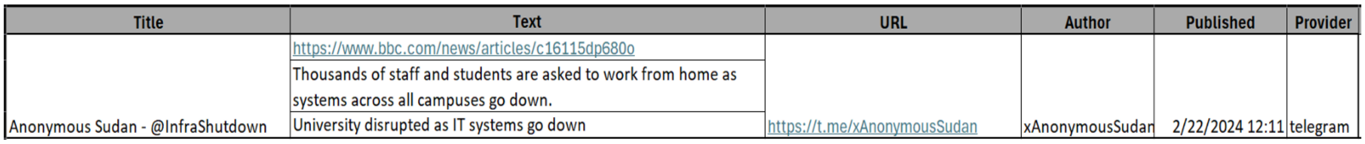
Figure 6. AS Targets

The Intersection between Cyberwarfare and Influence

To define influence, many factors must be considered. Influence is causing an effect in an indirect way (Thomas, Thompson, & Wanless, 2020). For a cyber actor this can be weaponized both with their cyberattacks but also how they publicize their actions and the reasons behind them. Hacktivist is the term industry uses for cyber actors that specifically hack for a cause (Fortinet, n.d.). This subsection of cyber threat actors uses influence operations with many if not most of their technical actions.

Technical Operations

Cyber threat actors influence people and organizations directly through their technical operations – these are the physical effects of the action. The people affected, systems that had outages, data stolen or manipulated. For example, a powerful DDOS was used to affect outages across two-high profile U.K. universities in February 2024 (Lawson, 2024) *Anonymous Sudan* claimed the attack and stated their reason was due to "the U. K's continued support of Israel" (Jack, 2024). Cyber actions such as these have physical impacts on victims.

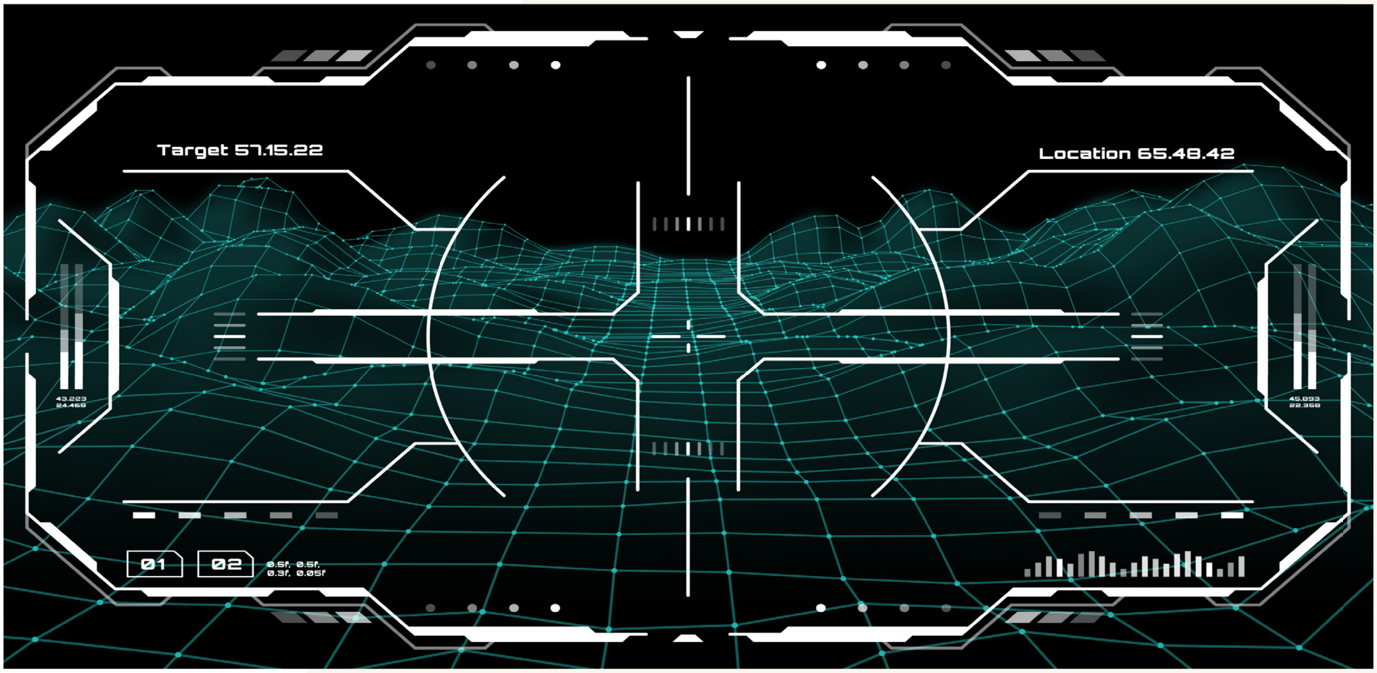


Title	Text	URL	Author	Published	Provider
Anonymous Sudan - @InfraShutdown	https://www.bbc.com/news/articles/c16115dp680o Thousands of staff and students are asked to work from home as systems across all campuses go down. University disrupted as IT systems go down	https://t.me/xAnonymousSudan	xAnonymousSudan	2/22/2024 12:11	telegram

Figure 7. message archive example of xAnonymousSudan's reposts of the BBC articles related to their attack (Perry, 2024)

Attacks like these can be used within a conflict to great effect. While any target can be fair game, hacktivists often target higher profile companies, institutions, and organizations. These are often big companies that are a part of that country's defense industrial base. Specifically *Anonymous Sudan* targeted big targets such as telecommunications, a big oil company, and a hospital (Perry, 2024). These targets have multiple things that make them good targets for cyber threat actors. These include possible financial gain, disruption of critical infrastructure, and better advertising for the cyber threat actor, or fame.

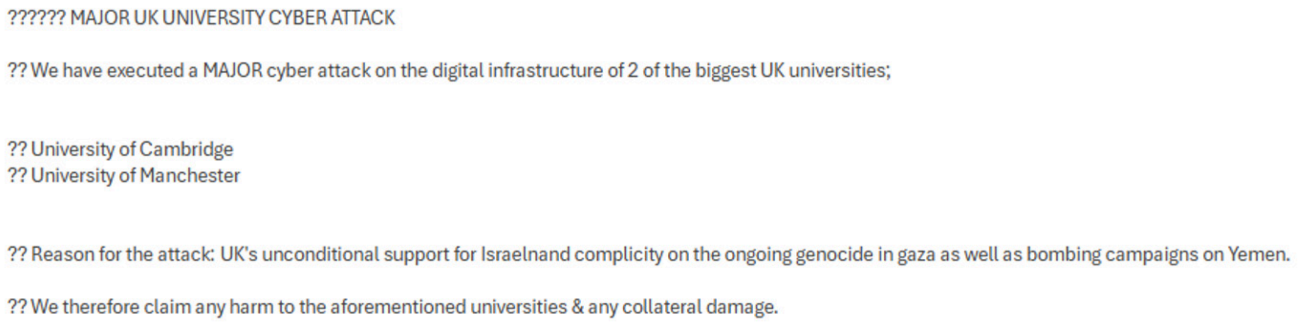
These are examples of the tangible effect of cyber warfare. There is a difference between the physical effect of the cyberattack and the effect that is cultivated by the actor. Independent cyber threat actors like *Anonymous Sudan* often use attacks that have an immediate effect. They use their attacks to not only have a tangible adverse effect on their victim but also to employ psychological operations to mold perception in their favor. This is the influence operations portion of the attack.



Social Media Influence

Cyber actors often use publication to claim attacks, sell Malware-as-a-service, or just to garner awareness for a cause. For example, Anonymous Sudan often makes statements regarding their attacks on Telegram. The early 2024 UK University attack mentioned earlier was posted about by the actor as seen in Figure 8. This post served as a claim and advertising for their actions. They also point out specifically the reason behind the attack, which was specifically asserted to be the U.K's support for Israel. News of the attack and its effects were posted from other, credible sources as seen in Figure 7 (Lawson, 2024). Anonymous Sudan then reposted news articles to provide even more context and credibility. This cycle shows how the threat actor can use publicity and social media to spread its narratives and support for its causes.

Social media is a great tool for instant visibility for these actors. It is a platform to spread ideas and products globally. Independent cyber threat actors and specifically the subsection of hacktivists need to have such a platform to spread their cause. Anonymous Sudan specifically utilizes Telegram to post anything from chill comments, their attacks, or updates on their attacks. Victims to cyberattacks lose money, credibility with their customers and, worst case scenarios, contracts and business. By the independent threat actor posting these attacks themselves, it can prematurely reveal the attack and its effects to customers before incident response can occur. It also adds to the credibility of the tools and skills of the independent cyber threat actor.


?????? MAJOR UK UNIVERSITY CYBER ATTACK

?? We have executed a MAJOR cyber attack on the digital infrastructure of 2 of the biggest UK universities;

?? University of Cambridge
?? University of Manchester

?? Reason for the attack: UK's unconditional support for Israelnand complicity on the ongoing genocide in gaza as well as bombing campaigns on Yemen.

?? We therefore claim any harm to the aforementioned universities & any collateral damage.

Figure 8. Anonymous Sudan posting their attack

Anonymous Sudan also takes advantage of social media to connect with other cyber threat actors. These include ones they work directly with like Killnet and its associated accounts or accounts they do not often interact with, such as WeRedEvilsOG. Looking at these account connections, a clearer picture of how these cyber threat actors work together, learn from each other, and improve becomes clearer. For example, *figure 9* shows that *Anonymous Sudan* has connected with Killnet, InfraShutdown, their malware-as-a-service, Skynet, another botnet, and others like those.

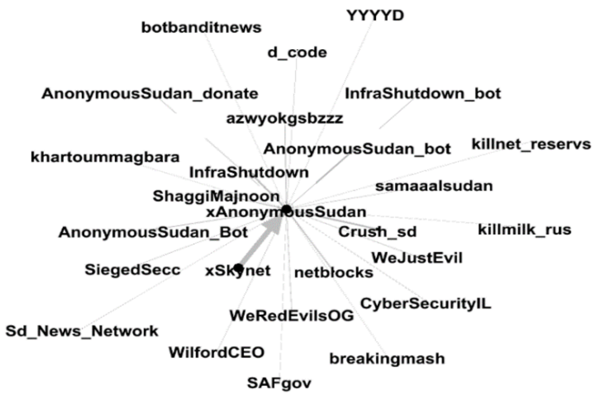


Figure 9: AS Telegram connections (Perry, 2024)

Influence-for-Hire and Revenue

One of the major differences between state-based actors and independent cyber threat actors is the need for money. State-based actors, often called APTs (advanced persistent threats), do not need this source of revenue as their actions are supported by their country of origin. Oftentimes this also means they don't need advertising and social media presence of independent threat actors either.

Independent threat actors often run a pseudo business model with malware or cyberattack tooling. This is so that they can afford tools and other specialized software. Anonymous Sudan utilizes their attacks to sell a DDOS-as-a-Service called InfraShutdown (What is a denial-of-service (DoS) attack?, n.d.). They have used and sold this service since entering the Israel-Hamas conflict. InfraShutdown is a distributed denial of service tool (DDOS). Denial of service is a particular type of cyberattack that sends empty traffic or packets to a web server to disrupt normal traffic from reaching that site. Anonymous Sudan specifically "promotes the new service through advertisements and by claiming denial of service attacks against highly visible and public targets" (Operator, 2024).

Workflow

Anonymous Sudan uses several tactics in their influence operations in combination with their cyberattacks. This workflow goes through several phases. First the attack itself, often the actual DDOS attack. In cyber operations against Israel, common targets have included academia and industry of other countries that support Israel. Stage 2 is the publication of the successful attack. Telegram or X are big platforms for quickly spreading information. *Anonymous Sudan* enjoys thousands of followers on their several accounts. This is often followed up with more posts on the effectiveness of the attack or other news reports on the cyberattack for effect. *Figure 10* shows how *Anonymous Sudan* works to combine their cyberattacks with influence to effect the perception of their causes. They utilize their own social media and cyberattacks, and to improve credibility, source news articles, other actors attacks, and other tangible effects of their actions and reposts them.

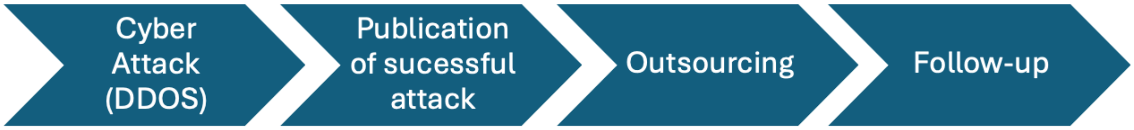
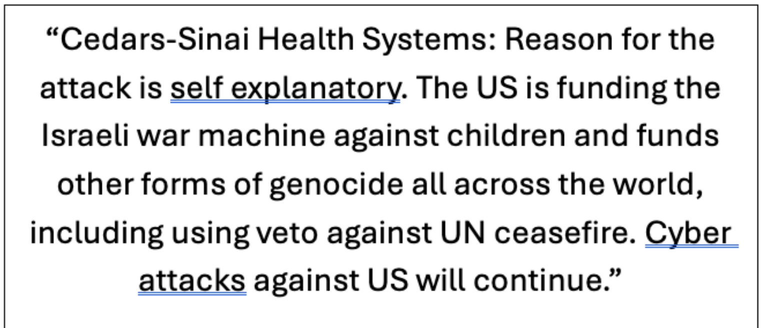


Figure 10. Workflow

A critical part of these posts is the sentiment expressed. Sentiment and word usage can shift perspective on a cyber action. When conducting sentiment analysis, especially when looking at kinetic conflicts, it's important to look for words that show subjective information (Gupta, 2018). The right words can change a cyberattack from an attack that affected hundreds to a righteous course of action for a worthy cause. The second critical part of these posts, which isn't immediately obvious, is how they disseminate them. *Anonymous Sudan* utilizes a few social media accounts to disseminate information, updates, and advertisements to a trusted group of followers (Operator, 2024). These accounts and channels provide the backbone of their ability to control the perception of their actions.

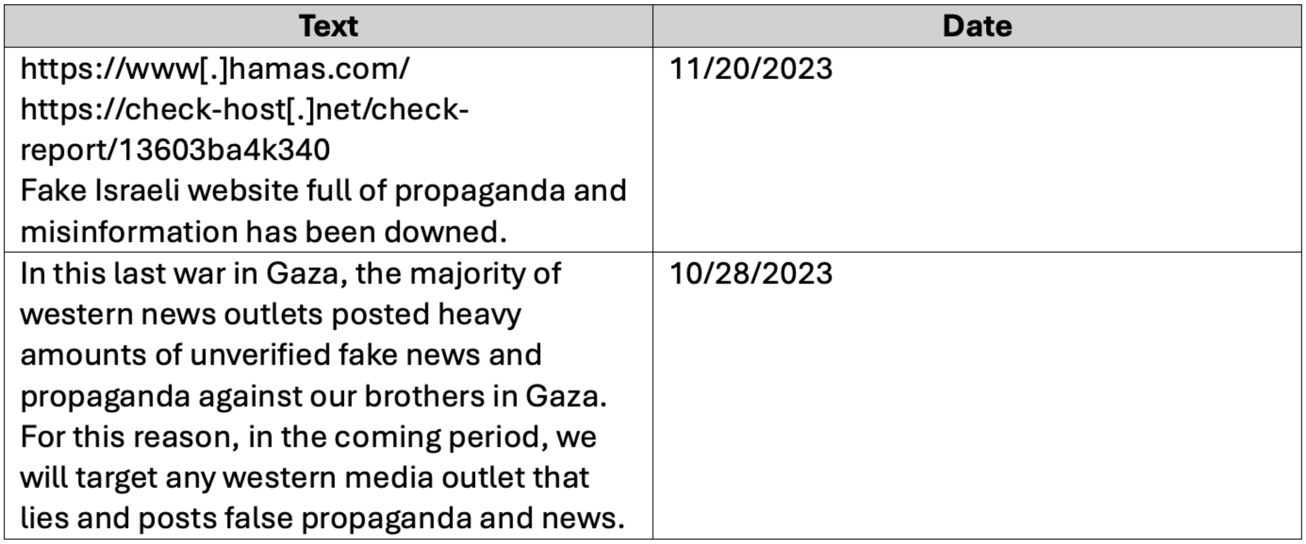
Disinformation campaigns have been used for propaganda in modern warfare for a bit now. In a research project completed by the University of Oxford in 2021, it wrote that "Social media platforms continue to play a critical role in the sharing […] communication for over a billion people around the world" (Samantha



"Cedars-Sinai Health Systems: Reason for the attack is self explanatory. The US is funding the Israeli war machine against children and funds other forms of genocide all across the world, including using veto against UN ceasefire. Cyber attacks against US will continue."

Figure 11. Example for Sentiment Analysis

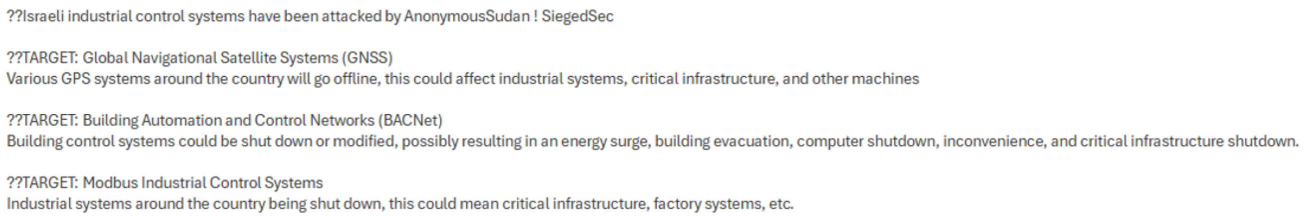
Bradshaw, 2021). Communication and manipulation is becoming more and more common online. Cyber influence operations "erode trust, increase polarization, and threaten democratic processes" (Microsoft Digital Defense Report, 2022). In fact, cyber influence operations includes this subsection of cyber-enabled influence operations. Iran is an example of how state-based threat actors got involved in the conflict in this way. These attacks aim to intimidate Israelis, criticize the government, destabilize Israel via polarization, and to undermine support to Israel (Intelligence, 2024). Anonymous Sudan does this but from the unique perspective of an independent cyber threat actor. For example, they would attack websites and news outlets that posted "fake information.". This may seem like a good thing, especially to those who agree with their cause. As a non-state actor, Anonymous Sudan has more flexibility in what they usually target, their objectives of each attack, and are able to communicate on social media more directly.



Text	Date
https://www[.]hamas.com/ https://check-host[.]net/check-report/13603ba4k340 Fake Israeli website full of propaganda and misinformation has downed.	11/20/2023
In this last war in Gaza, the majority of western news outlets posted heavy amounts of unverified fake news and propaganda against our brothers in Gaza. For this reason, in the coming period, we will target any western media outlet that lies and posts false propaganda and news.	10/28/2023

Figure 12. AS pledges against disinformation

Hacktivism is a type of cyber actors that hack for a cause. Oftentimes this includes other gains for the actors such as financial gain and fame on top of the additional support and visibility. *Anonymous Sudan* is considered a hacktivist. However, in a conflict these actions boil down to supporting a side. While these actors are not physically in the fight, their actions often have immense consequences in the conflict. It's important to understand a cyber threat actor to understand how they might get involved and change the conflict. Cyber threat actors target a number of different targets. As mentioned earlier, *Anonymous Sudan* itself targeted several different companies, countries, and sectors in the Israel-Hamas conflict. When key sectors are disrupted, this can cause a lot of damage to an actor in a conflict. Another independent cyber threat actor, SiegedSec, mentioned *Anonymous Sudan's* attack on Israeli infrastructure as seen in *figure 13*.



??Israeli industrial control systems have been attacked by AnonymousSudan ! SiegedSec

??TARGET: Global Navigational Satellite Systems (GNSS)
Various GPS systems around the country will go offline, this could affect industrial systems, critical infrastructure, and other machines

??TARGET: Building Automation and Control Networks (BACNet)
Building control systems could be shut down or modified, possibly resulting in an energy surge, building evacuation, computer shutdown, inconvenience, and critical infrastructure shutdown.

??TARGET: Modbus Industrial Control Systems
Industrial systems around the country being shut down, this could mean critical infrastructure, factory systems, etc.

Figure 13. Repost by xAnonymousSudan from SiegedSec (Perry, 2024)

Future

Understanding cyber threat actors, their targets, their motivations has always been important. As more independent malicious groups become more involved globally in conflicts it adds yet another layer to kinetic situations. Sentiment analysis or dissemination analysis of these threat actors' posts can be a gateway to curbing their influence, defining these cybercrimes or hacktivist activities, and helping to minimize the effect of independent cyber threat actors. Of course, measuring the influence, and therefore, the danger of each cyber group is difficult but prioritizing the limitation of the influence of malicious actors, such as *Anonymous Sudan*, can help slow down or stop their malicious activities, especially those within conflict zones. How Anonymous Sudan utilizes this technique in the Israel-Hamas conflict now and in the future is a marker for how cyber threat actors and hacktivists could act. Meaning that more and more could become involved in true conflicts, outside of their own country or main interests.

Conclusion

Cyber warfare is an emerging form of conflict. How cyberattacks are perceived is critical in a globalized world. Independent cyber threat actors use a number of methods to control outside perception of their actions in order to influence people about their causes, and gain fame and fortune. How a cyber operation is perceived can influence future operations, how the conflict is viewed, how the actor is viewed, or even create opportunities for the threat actor that would not have been there previously. This is critical for creating countermeasures especially against independent threat actors and hacktivists. Understanding the tactics, techniques, and procedures of these actors can lead to a wealth of knowledge, mitigation techniques, and better understanding of conflicts. Globalization means that information is spread at a faster rate than ever before Anonymous Sudan was using perception in their cyberattacks to generate influence for their cause in the Israel-Hamas conflict. Influence is not easily quantified, but understanding how it is generated in cyberwarfare and the control perception is the first step to protecting against influence operations in future conflicts.

References

Microsoft Digital Defense Report. (2022). Retrieved from Microsoft: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/microsoft-digital-defense-report-2022.pdf?culture=en-us&country=us

Anonymous Sudan. (n.d.). Retrieved from radware: https://www.radware.com/cyberpedia/ddos-attacks/anonymous-sudan/

Cyber Aggression Rises Following the October 2023 Israel-Hamas Conflict. (2023, October 11). Retrieved from radware: https://www.radware.com/security/threat-advisories-and-attack-reports/cyber-aggression-rises-following-the-october-2023-israel-hamas-conflict/

Fortinet. (n.d.). *Hacktivisim Definition*. Retrieved from Fortinet: https://www.fortinet.com/resources/cyberglossary/what-is-hacktivism

Gatlan, S. (2023, November 9). *Cloudflare website downed by DDoS attack claimed by Anonymous Sudan*. Retrieved from bleepingcomputer.com: https://www.bbc.com/news/articles/c16115dp680o

Gupta, S. (2018, January 7). *Sentiment Analysis: Concept, Analysis and Applications.* Retrieved from towardsdatascience: https://towardsdatascience.com/sentiment-analysis-concept-analysis-and-applications-6c94d6f58c17

Intelligence, . T. (2024, February 26). *Iran surges cyber-enabled influence operations in support of Hamas.* Retrieved from Microsoft: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas

Jack, P. (2024, February 22). *U.K. Universities Targeted by Cyberattack*. Retrieved from insidehighered: https://www.insidehighered.com/news/global/2024/02/22/uk-universities-targeted-cyberattack-supporting-israel

KillNet Group. (n.d.). Retrieved from Blackberry: https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/killnet

Kozlovski, N. (2024, January 10). *Israeli cyber frontlines: Inside the digital warfare of the war with Hamas - Analysis*. Retrieved from The Jerusalem Post: https://www.jpost.com/israel-hamas-war/article-781682

Lawson, E. (2024, February 21). *University disrupted as IT systems go down*. Retrieved from BBC: https://www.bbc.com/news/articles/c16115dp680o

Najafimehr, M. (2022, April). *Figure - available from The Journal of Supercomputing*. Retrieved from researchgate.net: https://www.researchgate.net/figure/A-diagram-of-a-DDoS-attack-performed-with-a-botnet_fig1_357168204

Operator, I. A.-f.-H. (2024, February 28). Retrieved from radware: https://www.radware.com/security/threat-advisories-and-attack-reports/infrashutdown-anonymous-sudan-partners-with-ddos-for-hire-operator/

Perry, M. (2024). Anonymous Sudan Message Archive.

Samantha Bradshaw, H. B. (2021). *Industrialized Disinformation 2020 Global Inventory of Organized Social Media Manipulation*. Retrieved from University of Oxford: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf

SiegedSec. (n.d.). Retrieved from malpedia: https://malpedia.caad.fkie.fraunhofer.de/actor/siegedsec

Staff, J. P. (2023, April 27). *Israeli cyber security website briefly taken down in cyberattack*. Retrieved from jpost.com: https://www.jpost.com/breaking-news/article-736351

Staff, T. (2023, April 26). *Websites of Israeli port hacked; Sudanese group said to claim responsibility*. Retrieved from www.timesofisrael.com: https://www.timesofisrael.com/websites-of-israeli-port-hacked-sudanese-group-said-to-claim-responsibility/

Thomas, E., Thompson, N., & Wanless, A. (2020, June 10). *The Challenges of Countering Influence Operations*. Retrieved from carnegieendownment: https://carnegieendowment.org/research/2020/06/the-challenges-of-countering-influence-operations?lang=en

Vandersmith, O. (2023, March). *How Open-Source Intelligence Is Changing Warfare*. Retrieved from www.usni.org: https://www.usni.org/magazines/proceedings/2023/march/how-open-source-intelligence-changing-warfare

What is a denial-of-service (DoS) attack? (n.d.). Retrieved from Cloudflare: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

Acknowledgements

To my mentor, Mark Perry, for all his help!

Glossary

DDOS: Distributed Denial of Service or a type of cyberattack that floods websites with unimportant traffic so that it shuts down to legitimate traffic.

Independent cyber threat actor: A cyber threat actor who attacks, steals, disrupts normal cyber operations but is not directly endorsed or supported by a nation-state or government.

APT: Advanced Persistent Threat. Another name for state-based cyber threat actors
Edgelist: a scraped copy of telegram channels and their contents.

Message Archive: scraped data from Telegram showing the messages to and from certain users

Hacktivist: Hacktivism happens when political or social activists use computer technology to make a statement supporting one of their causes

PH
MODE -
10
POSITI
POSITION -
TEXT

The Richard S. Schultz '60 Symposium Fellowship was established in 2017 as an endowed fund in honor of “Dick” by his wife of fifty years, Myrna L. Schultz, their children, Marni and Alan, and his classmates and friends.

The fellowship enables Norwich undergraduates, from any academic discipline, the opportunity to pursue areas of inquiry and experiences that will promote and expand their understanding of the past and how it impacts the present and future. Through research, travel, and inquiry the Schultz Fellow and faculty advisor will offer perspectives for us to face the future with better understanding and confidence.

After a wide solicitation and competitive selection process, this annual fellowship is granted by the Norwich University Peace & War Center to an undergraduate student for a single project that may involve additional Norwich undergraduate students. The award includes a $3,500 grant.

N
1819
NORWICH™
UNIVERSITY

Norwich.edu