Retaining & Reintegrating the IT Army of Ukraine

2024

Prepared by :

Lindsay Dickinson, MPP Candidate

UVA | FRANK BATTEN SCHOOL of LEADERSHIP and PUBLIC POLICY

Table of Contents

Acknowledgements:

I want to thank the Batten School for providing me with two additional years to pursue my passions. Being welcomed into a community where faculty and staff are so willing to get to know their students and see them succeed was invaluable, and I will forever treasure your continuous support for my academic, athletic, and professional success.

I would like to thank Professor Pennock and Professor Myung for their mentorship and guidance throughout this APP process. I cannot express how much I learned from both of you, and I greatly appreciate the time you took at every roadblock to ensure I was set up for success.

To my fellow group members, Margaret Sparling, Kayvon Samadani, and Ky Schardein, the completion of this report would not have been made possible without your advice, feedback, and continuous support.

To my family – Michele, Jack, and Tim – thank you for being my biggest cheerleaders. Your unwavering support in all aspects of my life has never made me doubt my ability to achieve my goals and pursue my passions. I love you very much.

Lastly, to my friends – I cannot thank you enough for making Charlottesville my home these past two years. You truly embody what it means to be a leader and have brightened my life beyond measure. I cannot wait to see all that you accomplish.

Dedication:

This Applied Policy Project is dedicated to my Pop Pop, who I know would have been so excited to see me graduate this May. Thank you for instilling in me a continuous pursuit for learning, a pride in hard work, and an unwavering love for family and friends. I love and miss you very much.

Disclaimer:

The author conducted this study as part of the program of professional education at the Frank Batten School of Leadership and Public Policy. This paper is submitted in partial fulfillment of the course requirements for the Master of Public Policy degree. This report is a sole reflection of the analysis and conclusions of the author, which is not endorsed by the Batten School, the University of Virginia, or any other organization.

Honors Pledge:

On my honor as a student, I have neither given nor received aid on this assignment.

Key Acronyms:

Acronym	Definition
CBO	Congressional Budget Office
CISA	Cybersecurity and Infrastructure Security Agency
DDoS	Distributed Denial of Service Attack
DoD	Department of Defense
HFO	Hunt Forward Operation
IT	Information Technology
ITU	International Telecommunication Union
USAID	United States Agency for International Development

Key Terminology:

Term	Definition
Critical Infrastructure	"16 sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital that their incapacitation or destruction would have a debilitating effect on national security, economic security, public health or safety, or any combination thereof" (CISA, 2024).
Distributed Denial of Service (DDoS) attack	"attacker floods a server with internet traffic to prevent users from accessing connected online services and sites" (Fortinet, 2024)
Hacktivist:	"an individual that engages in political or social activism to make a statement supporting one of their causes" (Fortinet, 2024)
Malware	"software installed on a computer without the user's content and that performs malicious actions, such as stealing passwords or money" (McAfee, 2024).
Phishing	"by masquerading as a reputable source with an enticing request, an attacker lures in the victim in order to trick them … into taking some action that benefits the attacker" (What is a phishing attack, 2024).
Ransomware	

Social engineering techniques	"uses psychological manipulation to trick users into making security mistakes or giving away sensitive information" (What is social engineering, 2024).
Zero-day vulnerability	"cyberattack … that takes advantage of an unknown or unaddressed security flaw in computer software, hardware, or firmware" (What is a zero-day exploit, n.d.).

Executive Summary:

Immediately following Russia's invasion in February 2022, the Ukrainian government became the first nation-state to actively call upon global hackers to join its defensive and offensive military operations (Karagiannopoulos, 2023). Known as the IT Army of Ukraine, this loosely affiliated hacker group has quickly pioneered a new vision for cyberwarfare and cyber defense due to its success in the current conflict. Despite its success, the IT Army's current structure and methods of operation blur the line between combatants and civilians, posing a threat to public safety. Moving forward, it is imperative to provide the Ukrainian government with formal avenues to retain and reintegrate the IT Army that simultaneously enable its members to continue to test and enhance their skillsets absent a threat to the general public.

This analysis will draw parallels from successful demobilization and reintegration strategies to provide IT Army members with effective public and private sector pathways for cyber skill retainment. Ensuring that the retainment and reintegration of IT Army members will enhance the defensive cyber capabilities of Ukraine requires an evaluation of five policy alternatives:

1. Establish a Ukrainian Cyber Reserve
2. Private Sector Ethical Hacking – Penetration Testing
3. Private Sector Ethical Hacking – Red Team Operations
4. Creation of a Public Sector Bug Bounty Program
5. Creation of a Ukrainian Hunt Forward Team

Each policy alternative is evaluated using four criteria: (1) cost, (2) effectiveness, (3) end strength, and (4) political feasibility. All criteria, with the exception of cost and end strength, are measured on a high, medium, and low scale. An in-depth analysis of each policy alternative reveals Alternatives 1 and 3 as the best choice. These alternatives are highly effective at enhancing Ukrainian cyber defense, and they provide members with opportunities to hone their skillsets while supplementing their income. Implementing both alternatives is critical to facilitating greater public-private collaboration and providing the Ukrainian government with the means necessary to protect its long-term national interests.

Introduction:

Problem Overview:

Although the current Russian-Ukraine conflict is the first conflict to use cyber warfare as a primary component of military operations, determining what constitutes an act of war in cyberspace is still ambiguous (Render-Katolik, 2023). While this has allowed the Ukrainian government to organize a global IT Army to conduct destructive and destabilizing offensive attacks against Russian targets, such ambiguity has also led to the increase in destructive Russian cyberattacks without consequence.

Problem Statement:

Since its inception in 2022, the IT Army of Ukraine has conducted over 2,000 offensive cyberattacks against Russian infrastructure through its global network of over 500,000 volunteers (Kirichenko, 2023; Temple Raston & Powers, 2023). The failure to provide IT Army members with pathways to formally retain and reintegrate their advanced skillsets will negatively impact Ukraine's defensive cyber capabilities in the face of perpetual Russian threats.

Due to Ukraine's history of responding to Russian aggression, both militarily and in cyberspace, it is evident that the Russian cyber threat will not dissipate at the conclusion of the kinetic conflict. As a result, retaining and reintegrating the advanced skillsets of IT Army members as a first means of cyber defense is critical to protecting Ukraine's territorial and sovereign integrity against Russia's global threat to democracy.

Document Overview:

This report will first provide background on the history of Russian-Ukrainian cyber conflicts, the IT Army's origins, operational structure, and current legal challenges, as well as the need to retain and reintegrate these members in the face of perpetual Russian threats. The document will then analyze evidence of public and private solutions, highlighting both key takeaways and limitations to the literature. The report will then outline five proposed solutions, analyze those solutions against four criteria, and summarize findings in an outcomes matrix. The report will conclude with a final recommendation that details implementation steps and potential barriers.

Target Audience:

The ideal target audience for this report is an organization that seeks to promote cyberspace stability and cybersecurity to protect U.S. strategic national interests. Retaining and reintegrating the skillsets of IT Army hacktivists is critical to this mission, as enhancing capacity building and responsible state practice will allow the U.S. to continue to develop strategic partnerships with allied nations. It is imperative that relevant audiences address this issue in the immediate future, as delaying implementation until the conclusion of the current conflict will prove ineffective at substantially retaining and reintegrating IT Army members in a manner that enhances Ukrainian cyber defense.

Background:

The following paragraphs provide an overview of the history of Russia-Ukraine cyber conflicts, as well as the origins and operations of the IT Army of Ukraine. It will then describe the varying legal implications associated with managing the IT Army and conclude with an analysis of the perpetual Russian threat.

History of Russia-Ukraine Cyber Conflicts:

Although the Russian-Ukraine conflict represents the "first modern war to feature a major cyber warfare component," Ukraine has a longstanding history of responding to Russia's cyberattacks using hacktivists (Render-Katolik, 2023 & Przetacznik, 2022). Prior to their illegal annexation of Crimea in 2014, Russia launched a distributed denial of service (DDoS) attack against Ukrainian networks and communications services to distract from Russian troop movement. In response, Ukrainian hacktivists mobilized under the "Ukrainian Cyber Alliance" to take down Russian websites and leak sensitive information (Shore, 2022). From 2015-2016, Russia continued to conduct DDoS operations against Ukrainian call centers, energy distribution companies, and electric substations, leaving 230,000 Ukrainian customers without power for 1- 6 hours in cold winter months (Shore, 2022). Ukrainian hacktivists responded by leaking the email contents of Putin's close advisor, revealing the Kremlin's desire to "destabilize Ukraine, undermine the government, and orchestrate elections in their favor" (Shore, 2022). Russia continued to increase the scale and scope of malicious cyberattacks from 2016-2021, the most notable including Notpetya, which is considered to be history's most destructive cyberattack (Shore, 2022).

In the months leading to the invasion of Ukraine in 2022, Microsoft was the first to identify and report malware within Ukrainian government IT systems (Shore, 2022). Soon after, the Russian government utilized DDoS attacks to shutdown government websites, banks, and radio stations and utilized malware to wipe data from over 100 organizations in the finance, IT, and aviation sectors (Shore, 2022). Although Russia's repeated malicious cyberattacks against Ukraine generated no long-term damage, it did catalyze the nation's development of strong defensive capabilities prior to Russia's invasion in 2022.

IT Army Origins:

Recognizing its strong foundations in cyber defense, the nation quickly realized it lacked the offensive capabilities necessary to defend forward, catalyzing the decision to look outside its borders for assistance. In February of 2022, Ukraine's Deputy Prime Minister, Mykhailo Fodorov, called on volunteer hackers to join the IT Army and engage in offensive cyber operations against Russia (Soesanto, 2022). This call to action was published on Facebook and Twitter, with a link to a Telegram channel containing "operational tasks" (Soesanto, 2022). These tasks are continuously updated and include target lists and the method of attack (Soesanto, 2022). The use of Telegram is of note, as this site is on the dark web and is notoriously used by hackers to encrypt communications and ensure anonymity (Javers, 2023). While the Facebook and Telegram messages directly called on Ukrainian citizens, Fedorov's Twitter post was written in "plain English," suggesting his intentional call to an international audience (Soesanto, 2022).

To date, the IT Army has amassed over 500,000 volunteers ranging from sophisticated IT professionals to amateur hackers (Temple-Raston & Powers, 2023). Although not direct participants, additional hacker groups including Anonymous and the Belarusian Cyber Partisans are working with the IT Army to target Russian civilian infrastructure (Render-Katolik, 2023). Accurate membership of the IT Army is unknown, with initial estimates based on 300,000 subscribers to its Telegram channel (Soesanto, 2022). Recent interviews with known IT Army members, however, have revealed actual membership estimates of 500,000 (Render-Katolik, 2023; Temple Raston & Powers, 2023). As illustrated by these interviews, it is likely that an unknown number of sophisticated cyber actors are conducting offensive cyber operations against Russian infrastructure in addition to those subscribed to Telegram.

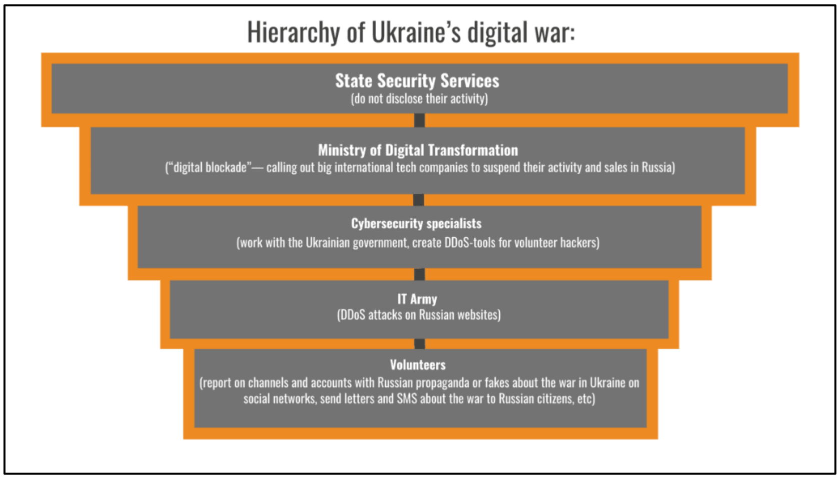

Hierarchy of Ukraine's digital war:
State Security Services
(do not disclose their activity)
Ministry of Digital Transformation
("digital blockade"— calling out big international tech companies to suspend their activity and sales in Russia)
Cybersecurity specialists
(work with the Ukrainian government, create DDoS-tools for volunteer hackers)
IT Army
(DDoS attacks on Russian websites)
Volunteers
(report on channels and accounts with Russian propaganda or fakes about the war in Ukraine on social networks, send letters and SMS about the war to Russian citizens, etc)

Figure 1: Hierarchy of Ukraine's Digital War
Source: The Record (Antoniuk, 2022)

IT Army Operations & Methods:

The IT Army primarily utilizes DDoS attacks to disrupt and destabilize Russian infrastructure (Shore, 2022). Operations are organized by about 30 Ukrainian government "Generals" and coordinated by IT Army "Colonels" - hackers with the greatest experience and skillsets, with successful operations promoted by Fedorov on social media (Kirichenko, 2023). Notable attack targets include Russian military equipment stores, banking systems, railways, and airline systems (Keary, 2023). In addition to conducting DDoS attacks, the IT Army has also conducted hack and leak campaigns, publicly revealing the documents of Russia's censorship and space agencies and a Belarusian weapons manufacturer (Shore, 2022). The purpose of these attacks is to (1) negatively impact public opinion, (2) undermine Putin's legitimacy, and (3) weaken Russian hackers by revealing communications and identities (Shore, 2022).

Legal Ramifications of Current IT Army Model:

The IT Army's capabilities and informal structure violate international law and incentivize Russian escalation. Although international law's applicability to cyberspace is contested, there are several clear applications that are currently being violated by the IT Army's organizational structure, as identified in the Tallinn Manual. Direct participation in hostilities as an organized group of combatants (OAG) has caused IT Army members to lose their civilian protections, primarily their inability to be targeted in an attack (Biggerstaff, 2023). The Tallinn Manual provides a specific example applicable to the IT Army, stating that civilian patriotic hackers that independently undertake offensive cyber operations against the enemy can be lawfully targeted by the enemy nation (International Group of Experts, 2017). As a result, the IT Army's current structure poses a critical threat to the safety and security of the public, as it provides Russia with the justification necessary to target civilian populations. Retaining and reintegrating IT Army members in a formal, legal structure will enhance Ukraine's defensive cyber capabilities in a manner that does not threaten public safety.

The Perpetual Russian Threat:

Russia will continue to pose an existential threat to the Ukrainian population due to the nation's inability to recognize Ukraine as an independent, sovereign nation (Costigliola, 2023). The Russian culture is rooted in pride and exceptionalism, which has strongly influenced its domestic and foreign policies (Kotkin, 2016). In the quest for a strong nation-state, Russia has often rejected alliances and agreements that did not place them as the prominent power (Kotkin, 2016). Such pride and exceptionalism have further fueled resentment towards the West, who have ignored Russia's security claims and "importance" in the global world order (Kotkin, 2016). The tension and animosity generated by this lack of acknowledgement, coupled with vulnerability felt by a lack of natural borders, often leads Russia to preemptively attack for its own security interests (Kotkin, 2016).

Since as early as 1948, U.S. officials have warned that Russia would never except Ukrainian independence (Costigliola, 2023). Not only do Russians and Ukrainians have close ethnic and economic ties, but Russia views Ukraine as a critical buffer between its own borders and the West (Costigliola, 2023; Mearsheimer, 2014). Russian leaders have expressed adamant opposition to NATO expansion, indicating that they would not stand for neighboring countries becoming "Western bastions" (Mearsheimer, 2014). Since powerful nations are typically sensitive to threats on their borders, Putin's vehement opposition to the alignment of Ukraine with the world's most powerful military alliance is not unreasonable (Mearsheimer, 2014).

Since no Russian leader will ever except a Western alliance with Ukraine, and Putin himself does not formally recognize Ukraine's territorial and sovereign independence, Ukraine is likely to face continued military and cyber threats (Costigliola, 2023). Interviews with IT Army members have revealed that Russia has constructed its own national offensive cyber program to teach skilled military students advanced offensive cyberattacks methods (Temple-Raston & Powers, 2023). Such programs have been differentiated into specific subjects and disciplines and are supported by a consistent stream of research and development (Temple-Raston & Powers, 2023). This program has fueled an increase in malicious cyber activity in the current conflict, which is likely to escalate as the program grows in scope and scale. As a result, fortifying Ukrainian cyber defense through the retention and reintegration of skilled IT Army members is critical to protecting Ukraine's territorial and sovereign integrity moving forward.

Evidence on Potential Solutions:

Ensuring that the skillsets of Ukrainian IT Army members can continue to be utilized is imperative to fortifying Ukraine's national cyber defense against adversarial threats. Drawing on lessons learned from existing public and private sector frameworks is critical to successfully retaining and reintegrating IT Army members within Ukrainian society.

Establishing A Formal Cyber Reserve

Creating a formal cyber reserve provides IT Army members with legal avenues to utilize their skills while providing greater transparency into a member's role as a civilian or combatant (Munive, 2016). Since hacktivism is less than 30 years old and the concept of creating a formal cyber reserve to specifically address hacktivism is novel, its success at retaining and reintegrating former hacktivists is relatively unknown (Grimes, 2016). Although nations with cyber reserves have effectively maintained their cyber defenses, it is unknown whether this is a direct result of the reserve's actions or from its classified operations.

The following sections detail two case studies for a Ukrainian cyber reserve.

Estonian Model: The Estonian Cyber Defense League (CDL):

The Estonian Cyber Defense League (CDL) is a subgroup of the Estonian Defense League, a volunteer national defense organization that resembles a combination of the U.S. national guard and a national militia (Cardash, 2013). As a formal reserve, volunteer members comprise an official chain of command, but often choose to participate separate from their professional jobs (Cardash, 2013). They do not receive pay and do not have strict participation obligations unless officially mobilized (Cardash, 2013). Although Estonia has not experienced a significant cyber incident since its inception, the CDL has been utilized during national elections and has participated in tabletop and tactical military exercises (Cardash, 2013).

Estonia's CDL provides flexible membership and easy mobilization, allowing its members to enjoy the monetary benefits of private sector employment (Cardash, 2013). Since the CDL does not have strict obligations for its members, individuals can scale participation as they see fit. Such flexibility, however, means that the CDL does not have the capacity to maintain 24/7 readiness or contribute to long-term missions (Cardash, 2013). Since many members hold private sector positions, members cannot commit to the long hours necessary to address acute crises (Cardash, 2013). Although comprised of highly skilled members, the CDL's flexible model prefers quantity over quality, and may not have the technical capabilities necessary to address immediate crises (Cardash, 2013).

U.S. National Guard Model:

U.S. National Guard Cyber reservists provide support at both the state and federal levels (Plamann, n.d.). Comprised of 3,900 reservists across 59 cyber units, National Guard members are required to complete one weekend of training per month and several weeks of active service per year (Plamann, n.d.; Siripurapu & Berman, 2024). As a result of this structure, members often hold civilian jobs or attend school while serving as a National Guard member and typically report to training in the state or locality of which they live (Siripurapu & Berman, 2024).

In addition to participating in U.S. government training exercises, such as Cyber Shield, Cyber Yankee/Dawn, and Cyber Flag/Guard, the National Guard provides its members with critical skills that are valuable in the private sector, including certifications in network security and ethical hacking (NGB Public Affairs, 2022; Army National Guard, 2024). Specifically identified in the 2016 National Cyber Incident Response Plan for its role in "information sharing, situational awareness, secure communications, and incident response," National Guard members effectively utilize skills learned in public and private sector roles to support the U.S. Department of Defense Cyber Mission Force (CMF) (Plamann, n.d.).

The U.S. National Guard traces its origins back to militias established by the American colonies (Siripurapu & Berman, 2024). Totaling 430,000 members, the U.S. National Guard can be mobilized by state governors and the President to respond to immediate emergencies and assist overseas missions (Siripurapu & Berman, 2024). Cyber reservists have recently provided immense support to state governments facing ransomware attacks, often conducting joint information sharing and capacity building cyber exercises with international partners through the State Partnership Program (Greig, 2023; Texas Military Department, 2023).

The National Guard is comprised of the Army National Guard and the Air National Guard and is overseen at the federal level by the National Guard Bureau (Siripurapu & Berman, 2024). The National Guard Bureau is operated by a 4-star general that is a member of the U.S. Joint Chiefs of Staff (Siripurapu & Berman, 2024).

Hunt Forward Teams:

Hunt Forward Teams are deployed at the request of partner nations and work in tandem with foreign cyber partners to search and remove malicious actors from network systems (Beecroft & Gilmore, 2023). In addition to identifying and removing threats, HFOs conduct intelligence assessments on adversarial behavior and share information with their respective governments and industry partners (Temple-Raston, 2023).

The structure of HFO operations is based on the U.S. Hunt Forward Team model. HFOs are defensive operations that analyze networks for suspicious activity and then evaluate that activity to determine if it is malicious (Temple-Raston, 2023). Once malicious activity is identified, teams will continue to search for similar threat signatures (Temple-Raston, 2023). Once the threat is sufficiently documented, Hunt Forward Teams will install unclassified equipment on partner nation systems and provide instructions for successful remediation (Temple-Raston, 2023). Hunt Forward Teams do not take steps to remediate the threat themselves and provide security recommendations based on previous HFO experience and industry standards (Temple-Raston, 2023).

The critical facet of HFOs is the intelligence collecting operation (Beecroft & Gilmore, 2023). At the permission of the partner nation, Hunt Forward Teams have returned to the U.S. with in-depth analyses of "malicious software" that have been incredibly useful for mitigating similar attacks on U.S. systems (Temple-Raston, 2023). HFOs enable nations to better identify malicious cyber activity and understand an adversary’s strategic calculus while simultaneously enhancing allied collaboration through assisting partner nations with critical network threat remediation (Temple-Raston, 2023).

Private Sector Employment Opportunities

As of 2022, there are about 600,000 unfilled cybersecurity positions, 560,000 of which are in the private sector (Rockeman, 2022). Due to the massive demand for cybersecurity professionals, the private industry has a direct incentive to actively participate in reintegration efforts due to the widespread benefits it will produce for the industry (Robinson, 2018). Although private organizations may express an unwillingness to assume the risks associated with hiring prior hackers into internal roles, private companies and security firms are likely open to employing these individuals as external contractors. Employing prior hackers as external contractors not only minimizes the risk associated with providing highly skilled hackers with internal access, but it also provides companies with the opportunity to proactively test their network for vulnerabilities. Known as “ethical hackers,” prior hacktivists can utilize their skills to externally hack networks, identify vulnerabilities, and provide recommended patches (Rudin, 2023). Providing prior hacktivists with a challenge, individuals can continue to employ their skills while earning generous compensation.

Analysis of Takeaways:

Based on the analysis of case studies and potential solutions, two primary takeaways are evident. The first takeaway is the difficulty in adopting kinetic solutions to the cyber context. Current gaps in international law, the lack of literature on this issue, as well as the ambiguity surrounding both public and private sector cyber operations make drawing applicable parallels difficult. Due to the rapid evolution of technology and malicious cyberweapons, it is evident that any solution recommended for implementation must be flexible and adaptable over time.

The second takeaway is that successful alternatives are often culture dependent. The U.S., Estonia, and Ukraine each have very different conscription structures, national perceptions of the military and public sector service, the scope and scale of operations, and the levels of public-private collaboration. Despite these differences, many alternatives are relatively successful because the programs were adapted to fit within the sociopolitical structure of their respective country. Ensuring that alternatives are implemented in a manner that both addresses Ukraine’s immediate security needs while fitting within the nation’s larger structure is critical for the long-term success.

Criteria:

The following policy analysis will assess five alternatives aimed at increasing the cyber capabilities of Ukraine's post-war society:

(1) Establish a Ukrainian Cyber Reserve
(2) Private Sector Ethical Hacking – Penetration Testing
(3) Private Sector Ethical Hacking – Red Team Operations
(4) Public Sector Bug Bounty Programs
(5) Ukrainian Hunt Forward Team

These policy alternatives will be evaluated according to four criteria: (1) cost, (2) effectiveness, (3) end strength, and (4) political feasibility. Each criterion, except cost and strength, will be evaluated using a high, medium, and low scale.

Cost:

Cost will measure, in U.S. dollars, the cost of program implementation for each policy alternative. Program implementation will include the cost of infrastructure, contracts, salaries, associated skills training, and operational costs associated with recruitment, including the processing of background checks and security clearances.

Effectiveness:

Effectiveness will measure the alternative's ability to enhance the defensive cyber capabilities of Ukraine. This criterion is critical, as it ensures that Ukrainian networks will remain resilient in the face of growing adversarial threats. Measuring Ukraine's defensive cyber capabilities will be achieved through the lens of cyber resiliency, defined by IBM using the following three assumptions:

(1) The policy alternative will enhance cyberattack prevention.
(2) The policy alternative will enhance the ability to withstand cyberattacks.
(3) The policy alternative will enhance cyberattack recovery and remediation efforts (IBM, n.d.).

A policy that meets all three assumptions will be high in effectiveness, a policy that meets two of the assumptions will be medium in effectiveness, and a policy that meets one or none of the assumptions will be low in effectiveness.

End Strength:

End strength will measure the alternative's ability to retain Ukrainian IT Army members. This will be measured by numerically counting the individuals employed under each policy. It is critical to retain the cyber talent of Ukrainian citizens to contribute to Ukraine's growing digital economy and provide legal pathways for IT Army members to utilize their skillsets in alignment with Ukraine's strategic objectives. Sincere there is evidence that hacktivists may turn to cybercrime to test and enhance their skillsets, ensuring that sufficient pathways are provided to these highly skilled and capable individuals is critical to enhancing Ukraine's defensive cyber capabilities (Antoniuk, 2024).

Political Feasibility:

Political feasibility will measure support for the alternative from Ukrainian officials, the U.S. government, IT Army of Ukraine members, and private stakeholders, when relevant. Measuring political feasibility will provide a greater understanding of stakeholder interest, which is critical for successful policy adoption and implementation. Political feasibility will be measured on a high, medium, and low scale. High political feasibility will have support from all stakeholders, medium political feasibility will have support from two stakeholders, and low political feasibility will have support from one stakeholder.

Gauging support amongst IT Army members and understanding the motivations underpinning their decision to engage in hacktivism ensures that these incentive structures can be mimicked across these policy alternatives. If IT Army members do not explicitly state support for the policy alternative, IT Army support will be assessed using the following three underlying assumptions:

(1) The policy alternative allows members to express patriotism.
(2) The policy alternative allows members to experience comradery and/or competition.
(3) The policy alternative allows members to test and enhance their cyber capabilities.

These assumptions are developed from research evaluating the underlying psychological motivations of hacktivists, which is provided in Appendix 1. Monetary gain will not be considered in this evaluation due to IT Army members' current participation in the conflict absent financial incentives.

Policy Alternatives

The following policy alternatives represent distinct reintegration pathways for Ukrainian IT Army members to pursue both public and private sector opportunities. Five alternatives aimed at increasing Ukraine's defensive cyber capabilities are as follows: (1) Ukrainian Cyber Reserve, (2) Private Sector Ethical Hacking – Penetration Testing, (3) Private Sector Ethical Hacking – Red Team Operations, (4) Public Sector Bug Bounty Programs, and a (5) Ukrainian Hunt Forward Team.

Ukrainian Cyber Reserve

Establishing a formal cyber reserve provides IT Army members with legal avenues to utilize their advanced skillsets. Providing reservists with flexible membership and easy mobilization, this model allows technical experts to enjoy private sector work while simultaneously using their volunteerism to express nationalist sentiments (Cardash, 2013). Since reservists are not paid a salary unless they are mobilized for active duty, there are no attendance obligations and individuals can scale participation as they see fit (Cardash, 2013). The Ukrainian Cyber Reserve will draw upon the best practices of Estonia's CDU and the U.S. National Guard Cyber Units.

Reserve positions require that individuals have previous experience and specialized expertise to minimize the length and costs of initial training (Baezner, 2020). Members must be at least 18 years of age, a Ukrainian citizen, and be able to pass a background check and security clearance (Baezner, 2020). IT

Army members that are not Ukrainian citizens or are citizens that hold dual citizenship cannot serve in the IT Army and will be directed to enlist in their respective host country's reserves.

Once accepted as a reservist, members will undergo initial team training under the supervision of a permanent military officer to develop comradery and learn to work efficiently as a unit (Siripurapu & Berman, 2024). After this initial training, members will be required to undergo training one weekend every month (Siripurapu & Berman, 2024). Although the IT Army has demonstrated significant offensive capabilities, reserve members will act in a purely defensive capability, whether that be through strengthening networks or providing support during cyber emergencies.

Private Sector Ethical Hacking – Penetration Testing

IT Army members will serve as private contractors, using their advanced skillsets to conduct penetration tests (pen tests) to identify weaknesses in computer networks and offer recommendations to strengthen systems. These ethical hackers will follow the MITRE ATT&CK framework to guide their methodologies and approaches to simulating a realistic cyberattack against the organization (MITRE, 2024). Through this framework, pen testers can utilize the successful tactics of malicious actors to search for critical vulnerabilities and flaws in network systems. Pen testing will then conclude with a report detailing identified vulnerabilities, patches, and recommended next steps.

Private Sector Ethical Hacking – Red Team

IT Army members will serve as private contractors, using their advanced skillsets to conduct red team operations. Red teams may be hired by the Ukrainian government, the private sector, or allied governments to test both the strength of their networks and the readiness of their employees to recognize, adapt, and respond to simulated threats in real-time. Red team operators are not constrained in their method of attack so long as they do not cause irreparable damage to an organization's operating systems. Red team operators typically utilize phishing and social engineering techniques as their first means of attack to gain administrative access (Fortra, n.d.; Borges, 2024).

Through these simulated attacks, the Ukrainian government and private sector will better understand the strengths and weaknesses of their respective systems by identifying and patching vulnerabilities, improving remediation efforts, and recognizing areas to improve personnel response. Given that red team exercises can be conducted from any location, IT Army members will be placed into red team units based on their respective geographic location. Respective units will be paid a yearly salary by the company with which they are employed, and their companies will be funded through contracts extended by governments and additional private sector organizations.

Public Sector Bug Bounty Programs

Bug bounty programs, also known as vulnerability award programs, allow IT Army members to utilize their advanced skillsets with greater autonomy. In actively searching for exploits and vulnerabilities in government systems, bug bounties provide IT Army members with compensation and formal recognition for identifying zero-day vulnerabilities (Beretas, 2023). Program management and coordination can be contracted out to HackerOne or left for Ukraine's Better Regulation Delivery Office (BRDO) (Better

Regulation and Delivery Office, 2023). After determining which sector of the UAF will host the bug bounty program, specific program management will be left to Ukraine's Cyber Lab, developed and financed by EU partners (EEAS Press Team, 2022). The Cyber Lab will verify vulnerability reports, work to patch vulnerabilities identified as high or critical threats, and compile a final report analyzing the program's effectiveness.

Ukrainian Hunt Forward Team

IT Army Members will be recruited to serve as members of Ukrainian Hunt Forward Teams under the direction of Illia Vitiuk, the head of the cyber division of Ukraine's Foreign Intelligence Security Service (SZRU) (Temple-Raston & Powers, 2023). The U.S. government's close and continued collaboration with Vitiuk and this division on HFOs provide a clear avenue for greater information sharing and direction at the outset of operations. Such operations will prove critical to strengthening Ukrainian defense systems against unknown adversaries. Although the Ukrainian government has demonstrated its effectiveness at remaining resilient to Russian cyberattacks, gaining a greater understanding of the threat signatures of additional adversaries will be critical to fortifying Ukrainian cybersecurity long-term.

Findings & Analysis:

The following section will analyze each policy alternative according to the aforementioned criteria.

Alternative 1: Establish a Ukrainian Cyber Reserve

Cost:

This expected annual cost of operating a cyber reserve is about $12.6 million, based on the U.S. Congressional Budget Office (CBO) estimate of the authorization and operating costs of establishing a U.S. Civilian Cyber Reserve in the Cybersecurity and Infrastructure Security Agency (CISA) (U.S. Government Publishing Office, 2022). Proposed in 2022, the CBO estimates that implementation would cost $63 million from 2021-2026, subject to availability of funds (U.S. Government Publishing Office, 2022). Such costs cover recruitment and training efforts, as well as the salaries associated with mobilizing about 30 reserve members per year to serve for six-months in CISA appointed positions (U.S. Government Publishing Office, 2022). Once mobilized, members will receive $440,000 in salaries and benefits, which those currently working in CISA's Cyber Defense Teams (U.S. Government Publishing Office, 2022).

Included in this calculation is the cost of hiring 10 full-time staff members for program management (U.S. Government Publishing Office, 2022). An estimated $10 million will be devoted to covering the salaries of these full-time staff members as well as the funds necessary to recruit and train members from 2021-2026 (U.S. Government Publishing Office, 2022).

In the event that additional facilities need to be constructed for reserve operations, the Ukrainian government will incur an up-front cost of $20 million (Talaber et. al, 2020). These estimates are drawn from U.S. CBO cost estimates for the development of new infrastructure to support a U.S. Space National

Guard of similar scale (Talaber et. al, 2020). This up-front cost is not included in the $100 million annual operating cost estimate.

Effectiveness:

This alternative is high in effectiveness, as it meets each of the following three assumptions:

Assumption 1: Cyber reserves enhance cyberattack prevention.

As Estonia's most internationally visible component of its military, the reserve's creation and subsequent bolstering has successfully contributed to the nation's cyber deterrence, successfully enhancing cyberattack prevention (Oh, 2019). Although the CDL has not been mobilized to combat a cyberattack, the CDL's efforts in capability building and cybersecurity awareness have contributed to the nation's rise as the 5th best nation in cybersecurity based on the International Telecommunication Union's (ITU) global cybersecurity index (Griffiths, 2015; ITU, 2024). The reserve discovers hundreds of vulnerabilities per day, immediately passing on threat assessment information to service providers to facilitate greater public private collaboration in preventing cyberattacks (Kuik, 2023).

The cyber reserves of the U.S. National Guard offer additional models for effective cyberattack prevention. The Colorado National Guard has assisted the Colorado Secretary of State's Office of Information Technology on numerous occasions to prevent cyberattacks, often conducting network monitoring during elections (Dugas 2022; Colorado National Guard Public Affairs, 2021). Similarly, the Texas National Guard assisted 22 Texas counties affected by ransomware attacks in 2019 (Soucy, 2019). Counties that had previously worked with the Texas National Guard to address and remediate ransomware attacks were unaffected by these widespread attacks, as attackers were unable to get past network firewalls largely implemented by Texas National Guard members (Soucy, 2019).

These examples clearly indicate that cyber reserves effectively enhance cyberattack prevention.

Assumption 2: Cyber reserves enhance the ability to withstand cyberattacks.

Estonia's CDU has not yet been called upon in response to a real-world incident (RIA, 2023). As a result, its effectiveness in bolstering cyber defense in direct response to an incident is unknown (RIA, 2023). However, the cyber reserves of the U.S. National Guard have demonstrated a consistent, effective pattern in enhancing states' ability to withstand cyberattacks. Governors across the U.S. have called on National Guard cyber reservists at least 41 times to provide "response and remediation, cyber defense analysis, cyber incident response planning, security planning, threat assessment, and interagency planning" (Freed, 2021; Clarke, 2021).

Assumption 3: Cyber reserves enhance recovery from cyberattacks.

U.S. National Guard cyber reservists have effectively helped both states and partner nations recover from cyberattacks. In 2022, Montenegro was affected by a ransomware attack that impacted the services and functions of numerous government ministries (LaDue, 2024). Montenegro's partnership with the Maine

National Guard through the State Partnership Program facilitated the dispatch of 20 U.S. cyber reservists to “advise, assist, and recover critical government systems and processes” of the Montenegro government in as little as 2 weeks (LaDue, 2024).

Within the U.S., the National Guard has effectively enhanced cyberattack recovery in numerous states, most notably in Colorado and Louisiana. In 2018, cyber reservists in Colorado’s National Guard were deployed to get services back online and contain ransomware to ensure it didn’t impact public facing services (Freed, May 2019). In 2019, Louisiana National Guard Units were similarly deployed to aid public schools affected by ransomware to remediate the attack and recover systems taken offline (Freed, Nov. 2019). The National Guard was successful in getting affected systems back online.

This evidence indicates that cyber reserves are highly effective in enhancing the ability to recover from cyberattack.

Cyber reserves enhance cyberattack prevention.	Yes
Cyber reserves enhance the ability to withstand cyberattacks.	Yes
Cyber reserves enhance cyberattack recovery.	Yes

End Strength

This alternative is low in end strength. Although traditional reserves typically retain significantly more individuals than a nation’s standing military, cyber reserve membership has traditionally been much smaller, comprising an estimated 1.6% of the entire military reserve. For example, as of 2022 there are 4,000 cyber specific members of the 450,000 that comprise the U.S. National Guard (U.S. Cyber Command Pubic Affairs, Apr. 2022; Hughes, 2022). Although membership in cyber reserves will vary based on a nation’s size, available expertise, and the nation’s conscription model, evidence indicates that cyber reserves typically hold between 150 – 5,000 reservists at a time (Baezner, 2020). Since Ukraine currently holds 250,000 individuals in its military reserves, estimated membership for this cyber reserve is projected at 4,000 members, which fits well within the range of documented cyber reserve membership (The New Voice of Ukraine, 2023).

Political Feasibility

This alternative is high in political feasibility, as there is explicit support from all stakeholders.

The Ukrainian government is currently drafting legislation to make the IT Army a formal cyber reserve within the Ukrainian Armed Forces (Waterman, 2023). Natalia Tkachuk, the Secretary of Ukraine’s National Coordination Center for Cybersecurity, has released several public statements indicating broad support, as the formal cyber reserve solves three strategic issues for the Ukrainian government: (1) Preventing hackers from interfering with Ukrainian government cyber operations, (2) Reducing conflict expansion, and (3) clarifying combatant and civilian status for IT Army members (Waterman, 2023). Tkachuck expressed hope that the drafted law formalizing the reserve structure will be passed soon, as the cyber reserve would "become the basis for building the states cyber defense capabilities" (Waterman, 2023).

Although the U.S. has not publicly expressed support for the creation of a Ukrainian cyber reserve, existing evidence suggests that the U.S. will support its creation due to its collaboration with foreign cyber reserves and its commitment to its own National Guard cyber units. The U.S. National Guard frequently participates in exercises with the CDU, and the U.S. has put forward legislation with the hopes of creating its own formal cyber reserve within CISA (U.S. Cyber Command, Dec. 2020; U.S. Government Publishing Office, 2022). Since the U.S. has not passed such legislation, Ukraine's successful creation of a reserve can serve as a model for U.S. implementation.

The IT Army has expressed explicit support for the cyber reserve and the draft law that is currently in Ukrainian Parliament. Members "fully trust" that their interests will be well represented in the draft law and view the creation of the cyber reserve as helpful "in building a more effective defense against cyber threats" (Waterman, 2023).

Alternative 2: Private Sector Ethical Hacking – Penetration Testing

Cost:

On average, governments and organizations can expect to spend about $141,000 on pen testing. The average cost for a single network pen test of average to low complexity is $50,000 (Cole, 2024). Since surveys indicated that 85% of respondents conduct pen tests once a year, with only 39% of respondents conducting up to two tests per year, average annual costs for pen testing will represent the cost of the test itself (Digby, 2023). Cost can exceed or fall below this estimate depending on the scope of the pen test, the types of pen testing requested, the environment size, as well as the detail requested in the final report (Baran, 2023).

Average annual costs for pen testing include salaries, which is about $90,000 in the U.S. (Rijnetu, 2024). Entry level penetration testers with less than 1 year of experience typically receive a salary of about $70,000, while penetration testers with 10-19 years of experience earn a salary of about $121,000 (Rijnetu, 2024). These salaries are slightly lower in Europe, with penetration testers receiving starting salaries between $34,000 and $63,000 (Rijnetu, 2024).

Effectiveness

This alternative is medium in effectiveness, as it meets two of the following three assumptions.

Assumption 1: Private sector ethical hacking enhances cyberattack prevention.

Penetration testing is critical to preventing cyberattacks, as it simulates a malicious intrusion to preemptively identify and patch vulnerabilities within system networks and devices (What is penetration testing?, 2024). These intrusions are authorized by the system owners and can be broad or narrow in scope upon the owner's request (Coverage-Based Penetration Testing vs. Depth-Based, 2021). Although it is impossible to have a 100% vulnerability free system, proactively searching and remediating vulnerabilities allows hackers to identify likely attacks to the network and advise business owners of the proper steps necessary to enhances the overall system security. In one study, a pen test that scanned for about 18 hours across 1071 hosts identified 8,982 vulnerabilities, 230 of which were unique (Sorensen et. al, 2018). Results of this penetration test further identified that 11.58% of hosts had at least 1 critical vulnerability, 10.74% of hosts had at least 1 high vulnerability, and 63.21% of hosts had at least 1 medium vulnerability (Sorensen et. al, 2018). In providing owners with specific, actionable steps to enhance the security of their business, penetration tests effectively anticipate and prevent cyberattacks.

Assumption 2: Private sector ethical hacking enhances the ability to withstand cyberattacks.

Manual penetration testing is critical to ensuring that businesses can withstand cyberattacks. Although any business can purchase a tool or conduct a scan, hiring individuals that can think and mimic the attacks of malicious cyber actors is essential to ensuring that both network systems and IT professionals can withstand a "real-world adversary" (Penetration Testing, 2024). Manual penetration testing provides further benefits in comparison to automated tools because it identifies both existing threats and zero-day vulnerabilities, areas that threat actors often seek to exploit when conducting attacks. Furthermore, penetration testing accurately assesses the threat level of each vulnerability identified, as well as whether smaller threats may become critical if used in a "complex attack pattern" (Penetration Testing, 2024) In simulating the behavior of real-world adversaries, both from positions internal and external to the network, penetration testers effectively examine whether networks and businesses are "robust enough to withstand attacks" (Penetration Testing, 2024).

Assumption 3: Private sector ethical hacking enhances cyberattack recovery.

Penetration testing does not enhance cyberattack recovery. The purpose of the test is to identify and exploit vulnerabilities and provide patches via a formal report. Doing so instructs IT personnel on how best to prevent and prepare to withstand harmful cyberattacks and does not instruct personnel on how best to remediate and recover from cyberattacks.

This evidence indicates that penetration testing ranks medium in its ability to effectively enhance the defensive cyber capabilities of Ukraine.

Penetration testing enhances cyberattack prevention.	Yes
Penetration testing enhances the ability to withstand cyberattacks.	Yes
Penetration testing enhances cyberattack recovery.	No

End Strength

Penetration tests can typically be conducted by two to three individuals, although the number of penetration testers required to perform the project may rise due to three factors: requesting higher complexity penetration tests, large business size, and the complexity of an organization's infrastructure (Das, 2018; Infosec, 2024). In 2022, the U.S. had 27,409 unfilled penetration testing positions (Rijnetu, 2024). On average, 16,800 information security analyst positions are expected to open each year to directly replace those leaving the workforce (U.S. Bureau of Labor Statistics, 2023). As security breaches and data leaks among private corporations continue to rise, this present demand for penetration testers is only expected to increase (Infosec, 2024).

Political Feasibility

This alternative is medium in political feasibility, as there is explicit support from two stakeholders.

Since the inception of the Russia-Ukraine conflict, the Ukrainian government has revealed an increased willingness to collaborate with the private sector to enhance national cyber defense, especially in areas of vulnerability identification and remediation. Georgii Dubynskyi, the Deputy Minister of Digital Transformation of Ukraine, indicated through numerous public statements that Ukrainian collaboration and partnership with private companies has been critical to enhancing national cyber defense through information sharing and vulnerability identification (Pell, 2022).

Microsoft has been a key player in this arena, providing continuous sources of threat information, recommendations for improving Ukrainian cyber defense, and predictions of malicious Russian cyberwarfare based on pre-identified patterns (Krasznay, 2024). Such collaboration and public statements have been coupled with legislative action, as the Ukrainian legislature has amended its data protection laws to permit government authorities to move data into the public cloud (Kaushik, 2022). Based on the sophistication and skill level required for successful IT Army attacks, it can be reasonably ascertained that many IT Army members already have experience in the private sector and may be continuing to hold those positions while contributing to IT Army efforts.

The U.S. government relies heavily on the private sector to inform and enhance its cyber defense. Partnerships including the Joint Cyber Defense Collaborative (JCDC) have contributed to "cyber defense planning" and "effective government-industry coordination mechanisms" (Whyte, 2024). U.S. Cyber Command has additionally recognized the crucial role of private industry in informing national cyber defense priorities. To enhance collaboration and information sharing, U.S. Cyber Command created Under Advisement (UNAD), an unclassified program that allows industry partners to share technical information on identified foreign threats (Cyber National Mission Force Public Affairs, 2023; Sivesind, 2023). U.S. Army Major General William J. Hartman has specifically identified this program as "game changing" (Sivesind, 2023).

Since IT Army members have not explicitly stated their support for this policy, the following underlying assumptions will be utilized to determine IT Army member support for the policy alternative.

The policy alternative allows members to express patriotism.

The ability for IT Army members to express patriotism is highly dependent on the mission of the hiring company and the contract with that hiring company. IT Army members conducting pen tests to protect organizations from malicious actors are more likely to express patriotism than IT Army members conducting pen tests at the request of a company trying to meet compliance regulations. Similarly, IT Army members that work for companies contracted out by the public sector, such as Microsoft, are likely to express patriotism at a higher rate than companies that are only contracted out by the private sector.

The policy alternative allows members to experience comradery and/or competition.

Pen testing allows members to experience comradery and/or competition. Although pen testers' ability to develop comradery through teamwork depends on the company they are contracted out to, pen testing is quickly becoming a competitive field. As cyberattacks and data breaches continue to increase, both the public and private sector will continuously be looking towards the most capable pen testers to evaluate their company's security posture (Chan, 2024). Now that the cybersecurity profession is seeing an influx of professionals, pen testers will face increased competition to "stand out," whether that be through their performance, experience, certifications, or ability to remain calm in a high-pressure environment (Chan, 2024).

The policy alternative allows members to test and enhance their cyber capabilities.

Pen testing allows members to test and enhance their cyber capabilities within a specific framework. Many pen tests, in addition to following the explicit requests of the hiring organization, follow the MITRE ATT&CK framework (Find a Pentesting Provider That Uses the MITRE ATT&CK Framework, 2024). This framework, which serves as a global knowledge base of adversary tactics, provides a framework for pen testers to follow to conduct the attack (Find a Pentesting Provider That Uses the MITRE ATT&CK Framework, 2024). While pen testing does allow individuals to refine specific skills, it does not provide pen testers with the freedom to enhance skillsets outside of those specifically authorized by the hiring organization.

Alternative 3: Private Sector Ethical Hacking – Red Teams

Cost

The average annual cost for red team operations, including salaries, is $1.95 million. The average cost for red team operations can range from $50,000 to $150,000 depending on the size of the organization, the complexity of the network environment, and the threat level or sophistication of the attack requested (Baran, 2023). Since red team members operate as if they were malicious actors, individuals are compensated in a manner that matches the high level of skills required for the role. Furthermore, the high contract costs are reflective of the extended length of operations. Since many malicious actors, after gaining access, attempt to remain in the network undetected for as long as possible, the timeline required for red team operations typically exceeds that of traditional penetration tests. In the United States, the average salary for a red team penetration tester is about $120,000 (ZipRecruiter, 2024). Since red teams are typically composed of 8-15 members, the average annual salary for a red team of 15 members is $1.8 million (Evenden, 2020).

Effectiveness

This alternative is medium in effectiveness, as it meets two of the following three assumptions.

Assumption 1: Red Team operations enhance cyberattack prevention.

Red Team operations effectively prevent cyberattacks by testing the strength and capabilities of both an organization's networks and its IT personnel. Utilizing individuals with the skills, knowledge, and creativity to mimic a real-life threat actor provides organizations with greater opportunities to test for backdoors and vulnerabilities that could significantly threaten their system's security (Borges, 2024). Since these attacks occur without the IT personnel's knowledge, both red team actors and IT managers can evaluate the organization's capacity to "detect, prevent, and eliminate vulnerabilities," in response to a realistic threat (Borges, 2024). Identifying and evaluating areas of exploitation, both within systems and amongst personnel, is effective at preventing malicious actors from utilizing similar techniques to conduct cyberattacks (Borges, 2024).

Assumption 2: Red Team operations enhance the ability to withstand cyberattacks.

Red Team operations effectively enhance the ability to withstand cyberattacks. In a 2020 study conducted by Exabeam, red team exercises led 74% of organizations to increase investments in security infrastructure, with 18% making significant changes (Borges, 2024). Since red team operations mimic the behavior of a real-life threat actor, the process of red teaming enhances organizations' preparedness for real-world attacks and provides organizations with the opportunity to develop more effective response plans (Red teaming: Everything You Need To Know, n.d.). In addition to identifying network and system vulnerabilities, red team exercises train IT professionals on how to more effectively and efficiently recognize and mitigate cyberattacks (Red teaming: Everything You Need To Know, n.d.). By testing the resiliency of an organization's system and its employees, red team operations enhance the ability to withstand cyberattacks by minimizing the time it takes IT professionals to identify and respond to malicious behavior (Cole, 2022).

Assumption 3: Red Team operations enhance cyberattack recovery.

Red Team operations do not enhance cyberattack recovery. The purpose of red team operations is to mimic the tactics and behavior of a legitimate threat actor to test the security capabilities of an organization's systems and IT personnel (Borges, 2024). These tests are conducted to preemptively identify and remediate vulnerable areas or behavior that would threaten network security. As a result, enhancing cyberattack recovery efforts is not within red team operations' scope.

This evidence indicates that red team operations rank medium in its ability to effectively enhance the defensive cyber capabilities of Ukraine.

Red Team operations enhance cyberattack prevention.	Yes
Red Team operations enhance the ability to withstand cyberattacks.	Yes
Red Team operations enhance cyberattack recovery.	No

End Strength

Red Team operations are typically conducted by a team of 2 to 20 individuals (Fortra, n.d.). Like penetration testing, the size of the red team is highly dependent on the complexity of the operation, the complexity of the organization’s infrastructure, and the overall size and scale of the organization (Das, 2018). The small retention size of red teams is a function of the high skillsets necessary to effectively perform the role. Red teams are typically managed by a single operator that will execute the attacks or planned scenarios (EPAM Anywhere Editorial Team, 2024). These individuals are highly trained and typically have extensive experience in former penetration testing roles (EPAM Anywhere Editorial Team, 2024). Aside from the operator, red teams members are also highly skilled ethical hackers or subject matter experts with a wide variety of offensive cyber skills (EPAM Anywhere Editorial Team, 2024). Having a team with varying capabilities will ensure that red teams can perform numerous attacks mimicking various types of threats to adequately test the strength of an organization’s network and IT personnel (EPAM Anywhere Editorial Team, 2024).

Political Feasibility

There is high support for red team operations within the Ukrainian government. Although the Ukrainian government has not explicitly stated support for such operations, the Ukrainian government was a participatory member of the 2023 NATO Crossed Swords and Locked Shields Cyber Trainings hosted by the Cooperate Cyber Defense Center of Excellence in Tallinn, Estonia (NATO Allied Command Transformation, 2023). As two of the largest cyber defense exercises in the world, the exercises utilize red team operations to mimic the malicious attacks and techniques used by adversaries to enhance the resiliency of NATO members and additional participants (NATO Allied Command Transformation, 2023; NATO, 2023). Participants have noted that these exercises are critical to exposing critical vulnerabilities and providing lessons that members can then take home to their respective cyber units to better enhance national defense (NATO Allied Command Transformation, 2023).

The U.S. government utilizes red team operations to test the strength and resiliency of its own IT networks and personnel. The DoD recently released a Pentagon cyber assessment program to enhance the efficiency of its red team operations, explicitly mandating that cyber red teams must assess operational networks and serve as “force aggressors” to better replicate the capabilities, tactics, techniques, and procedures of known cyber threat actors (Graham, 2024). CISA similarly utilizes red teams to gain greater insight into the resiliency of their systems and personnel, citing that when properly conducted red teams are invaluable to improving an organization's security controls, operations, and defensive capabilities (*Red Team Operations and Adversary Emulation*, 2022). CISA further demonstrates the value provided by red team operations by publicly publishing the lessons learned from their own operations to enhance the security of the public (CISA, 2023).

Since IT Army members have not explicitly stated their support for this policy, the following underlying assumptions will be utilized to determine IT Army member support for the policy alternative.

The policy alternative allows members to express patriotism.

The ability for IT Army members to express patriotism is highly dependent on the mission of the hiring company and the contract with that hiring company. IT Army members conducting red team operations for private companies are less likely to express patriotism than those conducting red team operations for the public sector. Were companies to publish lessons learned from red team operations in a manner similar to CISA, members may be more likely to express patriotism if they feel they are contributing to national cyber resiliency rather than the resiliency of one company (CISA, 2023). Similarly, IT Army members that work for companies that are contracted by the public sector, such as Microsoft, are likely to express patriotism at a higher rate than companies that are only contracted out by the private sector.

The policy alternative allows members to experience comradery and/or competition.

Red team operations require comradery to be effective. Since red teams are often comprised of individuals with different skillsets, approaches, and experience, ensuring that members are working together effectively is critical for red team operations to effectively mimic the techniques of advanced threat actors (Razmi & Barlow, 2023). It is only through comradery that red team operations can work effectively to test the security of an organization's IT systems and personnel (Razmi & Barlow, 2023). Collaboration and comradery both within red teams as well as with IT personnel defending networks is further critical to ensure that vulnerabilities and additional lessons learned can be communicated to organizations in a manner that is beneficial and enables them to enhance their security posture (Razmi & Barlow, 2023).

The policy alternative allows members to test and enhance their cyber capabilities.

Red team operations allow members to test and enhance their cyber capabilities. Since red team operators are tasked with mimicking adversarial behavior to penetrating systems, hackers are given creative freedom to achieve operational goals so long as their actions do not harm the organization's systems. This allows members to continue to test and enhance their offensive cyber capabilities in a manner that simultaneously enhances the defensive posture of the hiring organization.

Alternative 4: Public Sector Bug Bounty Programs

Cost

The average bug bounty cost for program owners is $300,000 but can range between $250,000 and $800,000 depending on the complexity and scope of the program (DDS, n.d.; Hack the Pentagon, 2022). As a baseline, the U.S. Department of Defense's pilot bug bounty program, Hack the Pentagon, cost $150,000 to run when it was first deployed in 2017 (Kozub, 2017). Program operation costs include the cost of individual payouts to hackers, which typically range from $100 to $15,000, dependent on whether the vulnerability identified is a low, medium, high, or critical threat (HackerOne, 2024). As Ukrainian bug bounty programs increase in size and complexity, the Ukrainian government can expect to spend about $3 million dollars in contracts to bug bounty operation platforms (Kozub, 2017). This estimate is based on the U.S. DoD and GSA's recent contracts with HackerOne, the primary bug bounty platform for the U.S. government.

Effectiveness

This alternative is medium in effectiveness, as it meets two of the following three alternatives.

Assumption 1: Bug bounty programs enhance cyberattack prevention.

DoD's Hack the Pentagon program has discovered over 2,100 vulnerabilities since its initial inception, with an average of 34 vulnerabilities defined as critical or high vulnerabilities per program cycle (DDS, n.d.). The DoD has resolved over 25,000 vulnerabilities across all its bug bounty programs, saving $64 million and achieving close to 800% return on investment (*U.S. Federal; "Hack DHS" Program Successfully Concludes First Bug Bounty Program*, 2022). Hackers vetted to participate in the programs typically report vulnerabilities as early as 13 minutes into the program, averaging over 200 vulnerability reports submitted for review within the first 6 hours (HackerOne, 2024). So long as adequate reporting mechanisms are in place, bug bounty programs do identify vulnerable areas in networks for government personnel to patch. Identifying and ranking the threat level of these vulnerabilities allows governments to preemptively remediate areas potentially vulnerable to cyberattacks and enhances an organization's ability to prevent cyberattacks by incentivizing hackers to report vulnerabilities that they would otherwise use against an organization (O'Neill, 2017).

Assumption 2: Bug bounty programs enhance the ability to withstand cyberattacks.

Bug bounty programs enhance an organization's ability to withstand cyberattacks by searching for critical vulnerabilities used by adversaries to cripple networks (Harper, 2023). The DoD has specifically included rapid response capabilities within their bug bounty programs to allow hackers to hunt for specific vulnerabilities in public facing infrastructure across a 72-hour period (Harper, 2023). Hunting and patching these critical, high threat vulnerabilities is essential to enhancing a companies' ability to withstand cyberattacks. Since internal IT professionals often cannot keep up with consistently identifying and remediating new vulnerabilities, bug bounty programs allow organizations to mitigate high level threats identified by bug bounty hackers will continuing to allow their internal IT professionals to patch low to mid-level vulnerabilities (Carty, 2022). Additionally, since traditional IT professionals have their own biases and approaches to identifying vulnerabilities, having a consistent array of hackers with different perspectives that think and act like malicious hackers ensures that there will always be individuals available to search for critical vulnerabilities (Carty, 2022).

Assumption 3: Bug bounty programs enhance cyberattack recovery.

Bug bounty programs do not enhance cyberattack recovery. The purpose of bug bounty programs is to preemptively identify vulnerabilities, primarily those of high and critical threat levels, that could be later exploited by malicious actors. Although bug bounty programs enable organizations to test their network security and ability to withstand attacks, bounty programs do not provide support or remediation in the event cyberattacks impact network operations (HackerOne, 2024).

This evidence indicates that bug bounty programs rank medium in its ability to effectively enhance the defensive cyber capabilities of Ukraine.

Bug bounty programs enhance cyberattack recovery.	Yes
Bug bounty programs enhance the ability to withstand cyberattacks.	Yes
Bug bounty programs enhance cyberattack recovery.	No

End Strength

This alternative will retain about 178 IT Army members. U.S. DoD bug bounty programs have consistently received over 1,000 applications to take part in the program (HackerOne, 2024). Despite such high numbers of applications, the extensive vetting and monitoring process has reduced the number of applicants permitted to take part in the program from over 1,000 to an average of 178 members (HackerOne, 2024). Detailed analysis is provided in Appendix 2.

Political Feasibility

This policy alternative has high support from the Ukrainian government. In March of 2022, the Ukrainian Parliament made changes to the criminal code of Ukraine to decriminalize interference in public sector information systems so long as such interference was conducted with the intent to discover vulnerabilities (SSSCIP, 2022). These changes were made in direct response to cyberattacks on government websites in September 2021 (SSSCIP, 2022). Recognizing the need for additional assistance in discovering vulnerabilities, the Ukrainian Cabinet of Ministers adopted a proposal by the State Special Communications Service to launch a national bug bounty program (Tech Ukraine, n.d.). The pilot project is being implemented by the National Coordination for Cybersecurity at the NCCC in Ukraine with support from the U.S. Department of State (NSDC, 2020).

In addition to providing support for Ukraine’s bug bounty program, the U.S. government itself utilizes bug bounties to enhance its national cyber defense. Former Secretary of Defense Ash Carter, in addition to other DoD leadership, has indicated through public statements how critical bug bounty programs are to national defense (HackerOne, 2024). These statements have revealed the ways bug bounty programs have enhanced U.S. national security and provided DoD officials with more opportunities to learn from outside expertise (HackerOne, 2024).

Since IT Army members have not explicitly stated their support for this policy, the following underlying assumptions will be utilized to evaluate potential Ukrainian IT Army member support for the policy alternative.

The policy alternative allows members to express patriotism.

Bug bounty programs allow members to express patriotism, as they have been cited to provide hackers, who typically face barriers to military or government employment, with opportunities to serve their country (U.S. Army Cyber Command, 2022). Katie Moussouris, who assisted in launching both Microsoft’s first bug bounty program and the DoD’s Hack the Pentagon program specifically stated that “There was a great amount of patriotic motivation,” to participate in the program (Infosecurity Magazine, 2017). The opportunity to serve their country and express such patriotic sentiments has driven hackers to continue to support the program year after year (Infosecurity Magazine, 2017).

The policy alternative allows members to experience comradery and/or competition.

Bug bounty programs allow members to experience comradery and/or competition. The inherent structure of bug bounty program induces competition, providing hackers with a given timeframe to discover as many vulnerabilities in the network system as possible, with significant monetary prizes and recognition awarded upon successful completion. Such competition is enhanced by the vetting process. Shrinking the available pool of talent to the most highly skilled, highly capable ethical hackers induces competition to discover as many vulnerabilities as possible, especially those assessed as high or critical vulnerabilities.

The policy alternative allows members to test and enhance their cyber capabilities.

Bug bounty programs allow members to test and enhance their cyber capabilities. So long as hackers remain within the constraints established by the program, hackers are free to utilize and test whatever capabilities they deem necessary to penetrate system networks and identify critical vulnerabilities. The innate competition of bug bounty programs as well as the prospect of recognition and monetary rewards encourages hackers to think creatively and work efficiently to find vulnerabilities. Vulnerabilities in U.S. bug bounty programs are increasingly seeing decreased times to vulnerability identification with vulnerabilities now being discovered and reported in less than one minute (Lim, 2017).

Alternative 5: Ukrainian Hunt Forward Team

Cost

The U.S. Department of Defense is currently allocating $91.5 million towards Hunt Forward Operations (HFOs) for FY 2024 (Beecroft & Gilmore, 2023). This is a $15 million increase from FY 2023 as a result of HFOs demonstrated effectiveness (United States Department of Defense, 2023).

Effectiveness

This alternative is medium in effectiveness, as it meets two of the following three assumptions.

Assumption 1: Hunt Forward Teams enhance cyberattack prevention.

U.S. HFOs have successfully conducted over 50 deployments across 24 countries in 77 networks (Nieberg, 2023). Identifying over 90 forms of malicious software, U.S. HFOs have successfully prevented cyberattacks by imposing serious costs on the "time, money, and effort" of malicious cyber actors (Nieberg, 2023). Using Ukraine as a case study, the U.S. and Ukraine have jointly "shared over 5,000 indicators of compromise" through HFOs (Pomerleau, 2023). This has allowed the nations to defend forward and effectively prevent destructive cyberattacks (U.S. Cyber Command PAO, 2022). Gaining greater insight into adversarial tactics further allows partner nations to fortify their own networks and deter malicious cyberattacks using similar methods (Pomerleau, 2023).

Assumption 2: Hunt Forward Teams enhance the ability to withstand cyberattacks.

Hunt Forward Teams enhance the ability to withstand cyberattacks for all parties involved, as exemplified in the current conflict. In the months leading to Russia's invasion, U.S. Hunt Forward Teams deployed to Ukraine and worked in tandem with Ukrainian SBU cyber offers to identify over 90 pieces of unique malware in Ukrainian systems (Temple-Raston, 2023). Identifying and remediating this malware enabled Ukraine to withstand cyberattacks that would otherwise have crippled their critical infrastructure (Temple-Raston, 2023; U.S. Cyber Command Public Affairs, 2022). In addition to addressing these initial discoveries, the unclassified equipment left by the U.S. Hunt Forward Team provided Ukraine with greater visibility into its networks, enabling SBU operators to continue to identify malicious software and withstand damaging cyberattacks (Temple-Raston & Powers, 2023).

U.S. Hunt Forward Teams have conducted 11 operations across 9 different nations, providing the U.S. with information necessary to remediate malicious cyber activity in its own networks (U.S. Cyber Command Public Affairs, 2022). These efforts ultimately enabled the U.S. election system to withstand foreign interference during the 2020 presidential election (U.S. Cyber Command Public Affairs, 2022).

Assumption 3: Hunt Forward Teams enhance cyberattack recovery.

Hunt Forward teams do not enhance cyberattack recovery. Since the intent of HFOs is to preemptively identify and mitigate malicious activity, conducting recovery operations for systems damaged by cyberattacks is not within the Hunt Forward Team's mandate (Beecroft & Gilmore, 2023).

This evidence indicates that Hunt Forward Teams rank medium in its ability to effectively enhance the defensive cyber capabilities of Ukraine.

Hunt Forward Teams enhance cyberattack prevention.	Yes
Hunt Forward Teams enhance the ability to withstand cyberattacks.	Yes
Hunt Forward Teams enhance cyberattack recovery.	No

End Strength

End strength of Hunt Forward Teams typically varies based on partner nation capabilities and threat level perception but are typically comprised of 10-39 personnel. As of 2023, the U.S. currently utilizes 39 "cyberteams" that employ a total of 2,000 personnel – both military and civilian (Temple-Raston, 2023). It is critical to note that Hunt Forward Teams typically retain about 50% of previous operators across missions (Temple-Raston, 2023). Interviews with Major General William J. Hartman, Deputy Commander of U.S. Cyber Command, revealed that retaining Hunt Forward operators allows the force to build on the experience and knowledge gained from previous missions (Temple-Raston, 2023; General Officer Management Office, n.d.). This signals greater leadership development and the expansion of Hunt Forward Teams as they continue to recruit new members.

Political Feasibility

This alternative is high in political feasibility, as there is explicit support for the alternative from all stakeholders.

This alternative has high support from the Ukrainian government. From December 2021 to March 2022, U.S. Hunt Forward Teams deployed to Ukraine and conducted HFOs in close collaboration with Ukrainian partners. These operations were extremely effective at enhancing Ukrainian cyber defense in the months immediately prior to and after Russia's invasion by identifying malicious malware within existing systems, as well as providing the training, equipment, and additional information necessary to identify and remediate future malicious cyberattacks. In addition to fortifying Ukrainian national defense systems, both U.S. and Ukrainian personnel noted that such joint operations strengthened existing partnerships and allowed personnel to develop greater comradery out of the successful identification and remediation of malicious activity (Temple-Raston, 2023).

The U.S. further supports Ukraine's creation of its own Hunt Forward teams due to the "resounding success" of its own programs (Nieberg, 2023). Through HFOs, the U.S. has effectively eradicated malicious actors and malware in over 20 countries, strengthening global security and stability in cyberspace as well as U.S. partnerships (Nieberg, 2023). Since U.S. adversaries will often attack U.S. allies harder than the U.S. itself, partnering with these nations has further enhanced the quality and frequency of allied information sharing (Nieberg, 2023).

The IT Army of Ukraine is likely to support the creation of Ukrainian Hunt Forward Teams. George Dubynski, Ukraine's Minister of Digital Transformation, revealed a willingness to establish Ukraine's own Hunt Forward teams, stating that it was a "big mistake" to not "create a dedicated cyber force prior to the conflict's inception (Temple-Raston, et. All, 2023). Since Ukraine's Ministry of Digital Transformation has been hands on in the creation and organization of the IT Army of Ukraine, it can be assumed that IT Army members would support the creation of a Ukrainian Hunt Forward Team.

Outcomes Matrix:

The table below simplifies the ranking of the policy alternatives against each criterion.

	Cost	**Effectiveness**	**End Strength**	**Political Feasibility**
Alternative 1: Cyber Reserve	$12.6 million annually	High	~ 4,000 members	High
Alternative 2: Penetration Testing	$50,000 annually	Medium	~ 1-2 members per test	Medium
Alternative 3: Red Team Operations	$1.95 million annually	Medium	~20 members per team	Medium
Alternative 4: Bug Bounty Programs	$300,000 self-run annually; $3 million to contract out	Medium	~ 178 members	High
Alternative 5: Ukrainian Hunt Forward Team	$91.5 million annually	Medium	~2,000 members	High

Recommendation:

Implementing a formal cyber reserve in addition to hiring IT Army members as red team ethical hackers is the best retainment and reintegration strategy to enhance the cyber capabilities of Ukraine. Although implementing the cyber reserve is high in cost, it is lower in cost than Hunt Forward Operations and provides similar opportunities for IT Army members to serve their country. Creating a formal cyber reserve has the highest rate of retention in comparison to other alternatives. While the quality of this retention may be lower than those within a Ukrainian Hunt Forward Team or a bug bounty program, the training and certification opportunities afforded to cyber reservists will provide members with ample opportunities to learn on the job and close this existing skill gap. Overall, creating a formal cyber reserve is the most effective alternative at enhancing Ukraine's defensive cyber capabilities and retaining the greatest number of IT Army members. In addition to providing IT Army members with greater opportunities to hone their skills in service of their country, a formal cyber reserve provides greater clarification of the member's status in the conflict. Although the process of entering the cyber reserve would remove the anonymity of IT Army member identities, it would eradicate ambiguity as to whether the member was a civilian or a combatant.

Since IT Army reservists would serve voluntarily on a part-time basis, coupling this strategy with red team ethical hacking pathways will provide IT Army members with increased opportunities to hone their skillsets while supplementing their income. Although its effectiveness and retention is lower than bug bounty programs, it is unlikely that government officials would permit reservists to participate in a public bug bounty program that is intended to provide rewards and recognition to unknown hackers in the general public. Since bug bounty programs often benefit from new perspectives and insights, the Ukrainian government is likely to bar reservists from participating when searching for vulnerabilities and exploits within government systems may be a part of their everyday role.

In comparison to bug bounty programs, the revenue stream offered by private sector red team hacking roles is more consistent, as members would receive an annual salary versus having to compete for small monetary rewards. Although the effectiveness of this program is lower in comparison to other alternatives, this alternative will enhance public-private information sharing and provide the Ukrainian government with greater visibility into the identities and actions of IT Army members. Such visibility will allow the Ukrainian government to monitor former IT Army actions over time and intervene if they feel hacktivist actions are becoming too offensive or escalatory.

Overall, the combined implementation of these two alternatives will provide the greatest benefit to Ukraine's post-war society.

Implementation:

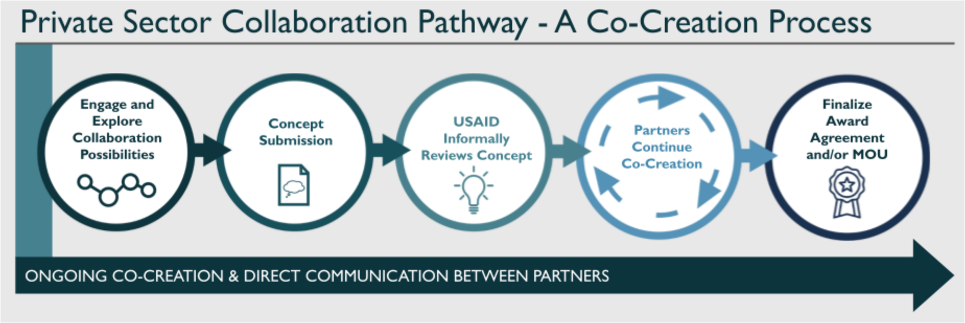
Cyber Reserve Implementation:

Creation of a formal cyber reserve must first be achieved by passing legislation through Ukrainian Parliament. Such legislation will be drafted by the Ministry of Digital Transformation to place the cyber reserve within the Ukrainian Armed Forces (UAF). Ensuring that the cyber reserve is placed neutrally as in the UAF, rather than situated under a specific military branch, will reduce “bureaucratic wrangling” by ensuring that one branch does not assume more power and funding (Waterman, 2023). Establishing a new position to head the Cyber Reserve force will additionally reduce tensions by ensuring that existing UAF leadership will not have to assume this role. This will ensure that current leadership can remain focused on the needs of their respective branches and that cyber reserve tasking is not skewed towards a specific branch. Looking to the U.S. model of assigning a high-ranking General to oversee this position will ensure that the Cyber Reserve is effectively managed and that the skills and capabilities of IT Army members can be broadly utilized across the UAF.

Private Sector Ethical Hacking – Red Team Implementation:

The Ukrainian government must first conduct a formal survey of the IT Army of Ukraine to determine exact membership and citizen status. Due to potential hesitancy from private sector employers to assume the risks associated with hiring former hackers, the Ukrainian government should establish public private partnerships with Ukrainian businesses. Not only will this strengthen Ukraine’s digital economy, but it will also assuage private sector concerns by ensuring hackers are properly vetted and approved by the Ukrainian government prior to beginning private sector work.

Ukraine’s Ministry of Digital Transformation should collaborate with USAID to develop a partnership pathway similar to USAID’s Private Sector Collaboration Pathway (Private Sector Collaboration Pathway, n.d.). Through this pathway, Ukrainian private sector businesses can more effectively signal both their capacity and willingness to hire former hacktivists. Following preliminary conversations, partners will formally submit a proposal to formally engage in a public-private partnership that generate hiring pathways for IT Army members. Similar to U.S. Veterans’ Preference and the current U.S. Federal IT/Cybersecurity Governmentwide Recruitment and Retention Authorities, this will incentivize former hackers to pursue private sector careers via this partnership due to the increased efficiency and ease of the hiring process.


Private Sector Collaboration Pathway - A Co-Creation Process
Engage and Explore Collaboration Possibilities
Concept Submission
USAID Informally Reviews Concept
Partners Continue Co-Creation
Finalize Award Agreement and/or MOU
ONGOING CO-CREATION & DIRECT COMMUNICATION BETWEEN PARTNERS

Potential Barriers to Implementation:

The primary barrier to policy implementation includes passing laws through Ukrainian Parliament. Although President Zelensky's implementation of martial law prevents Parliament from being impacted by external distracting factors, such as political rallies, protests, or shifting dynamics as a result of reelection campaigns, Ukraine has a history of being a "competitive country," filled with "contentious politics" (Goncharenko, 2023). Such contentious politics have led to an immense decrease in public trust of Ukrainian government institutions, which has been heightened in the past year by the firing of 2 senior defense officials in the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) for embezzlement of about $1.72 million in Ukrainian defense funds from 2020 - 2022 (Goncharenko, 2023; Antoniuk, 2023). Not only will the public demand heightened transparency in the drafting of new laws and programs, but there will also be heightened scrutiny in the processes necessary to allocate the funding necessary to implement the policies.

Additional barriers to policy implementation that Parliament will face is determining where these policies will be formally situated within the Ukrainian government. Due to the advanced capabilities and skillsets of IT Army members, placing this reserve force under the direction of a specific military branch or government agency will provide that entity with immense power. Statements by Tkachuk and foreign aid contractors working in Ukraine have already revealed such "bureaucratic wrangling", stating "There is friction between agencies … it's not a secret" (Waterman, 2023). Resolving such tensions by positioning the cyber reserve neutrally within the UAF, mimicking the National Guard model, will be critical to resolving these tensions and ensuring that the bill can be implemented effectively. Similarly, determining which additional agencies will be involved in the solidification of public-private partnerships is likely to induce additional "bureaucratic wrangling" (Waterman, 2023). Were the Digital Ministry of Ukraine to be the only stakeholder involved in the public-private decision-making process, the Ministry would have immense decision-making power to determine which agencies would benefit from these partnerships as well as which agencies would bear the costs.

A third barrier to policy implementation is the failure for IT Army members to mobilize when needed. Since these members are supplementing Ukrainian cyber defense systems on a voluntary basis, there is a risk that IT Army members will choose not to participate when mobilized due to ideological disagreements with leadership. This has occurred in Israel, as 300 cyberwarfare reservists previously issued a notice that they would not report for volunteer duty in response to Israeli government actions they viewed as unfavorable (Fabian, 2023). The ability for hacktivists to have the freedom to choose the extent of their participation may lead to the loss of critical skills necessary to support the nation in the face of severe cyberattacks. Understanding that these alternatives are a supplement to existing cyber skills will be critical to ensure that the Ukrainian government does not become overly reliant on IT Army members to address critical issues.

Appendix 1: Hacktivism Motivations

Understanding the psychological motivations underlying the IT Army's motivation to engage in hacktivism is crucial to generating tailored solutions to effectively retain and reintegrate their skillsets.

Patriotism:

Although hacktivism can be conducted individually, it is often conducted in groups via collective action in response to ideological motivations or patriotism (Romagna & Leukfeldt, 2023). Identifying with the group's values, the desire to participate in hacktivism reflects an innate desire to conform and achieve a sense of belonging and purpose (Romagna & Leukfeldt, 2023). A recent study interviewed 28 hacktivists to determine the primary motivators underlying hacktivist participation (Romagna & Leukfeldt, 2023). Identified in all interviews, the main motivator for engagement was "violation of moral convictions" (Romagna & Leukfeldt, 2023). Hackers detailed their desire to solve an issue, help others, and restore balance even if they were not the target of the violation (Romagna & Leukfeldt, 2023). Seeking to improve society and promote greater equality, hackers identified fighting crime/evil/terrorism and patriotism as two of the primary drivers for engaging in hacktivism (Romagna & Leukfeldt, 2023).

Camaraderie:

Social identity was the second driver in hacktivism participation, identified in 96% of interviews. Conforming personal identity to group identity was critical for hacktivists, as it provided a sense of belonging and meaning through shared values (Romagna & Leukfeldt, 2023). As a social activity, hacktivism generates feelings of peer recognition and respect, drives intellectual curiosity, and generates feelings of belonging by allowing individuals to participate within a team (Gaia et. all, 2020). Using "we" to describe actions, hacktivists presented clear connections with the values advocated by hacktivist groups, oftentimes motivated by political injustice and patriotism (Romagna & Leukfeldt, 2023).

Enhancing Skillsets:

Beveren's model of hacker development illuminates the ways curiosity and a desire to enhance one's skillsets motivate individuals to engage (Chng et al, 2022). According to Bevren's model, hackers enter the subject area with little to no skills, driven purely by their curiosity in the subject (Chng et al, 2022). As hackers gain greater experience and skills and become more engaged in the field, individuals begin to increasingly participate in hacktivism for the "intellectual challenge" (Australian Institute of Criminology, 2005). Rather than driven by external motivators such as recognition or financial rewards, these individuals are intrinsically driven to test their own merit (Australian Institute of Criminology, 2005).

Appendix 2: Bug Bounty Program Summary

The following table provides a summary of U.S. Department of Defense Bug Bounty Programs, spanning from 2016 to present. Summaries of each program include the number of vetted participants, the total number of valid reports, and the total payout to participating hackers in U.S. dollars. Averages of each program are used to inform the analysis of end strength for bug bounty programs.

U.S. Department of Defense: Bug Bounty Program Analysis			
	Vetted Participants	Total Valid Reports Received	Total Payout (USD)
Hack the Pentagon (2016)	250	138	$75,000
Hack the Air Force (2017)	300	207	$103,883
Hack the Army (2017)	371	118	$100,000
Hack the Pentagon 2.0 (2018)	19	65	$80,000
Hack the Air Force 2.0 (2018)	27	106	$103,883
Hack the Air Force 3.0 (2018)	30	120	$130,000
Hack the Army 2.0 (2020)	52	146	$275,000
Hack the Air Force 4.0 (2020)	60	460	$290,000
Hack the Army 3.0 (2021)	40	238	$150,000
Hack DHS (2022)	450	122	$125,600
Average:	~160	178	~ $134,336

Works Cited

Antoniuk, D. (2023, November 20). *Two top Ukrainian cyber officials dismissed amid embezzlement probe*. The Record from Recorded Future News. https://therecord.media/two-ukraine-cyber-officials-dismissed-amid-embezzlement-probe

Antoniuk, D. (2024, January 15). *Ukrainian arrested for infecting US Cloud Provider with cryptomining Malware*. The Record from Recorded Future News. https://therecord.media/ukraine-arrests-suspect-cryptojacking-cloud-resources

Army National Guard. (2024). *Enter the Newest Domain in Warfare*. https://nationalguard.com/careers/cyber

Australian Institute of Criminology. (2005). *Hacking motives*. Australian Government: Australian Institute of Criminology. https://www.aic.gov.au/sites/default/files/2020-05/htcb006.pdf

Baran, E. (2023, May 16). *Pricing Insights - How Much Does Penetration Testing Cost?*. Blaze Information Security. https://www.blazeinfosec.com/post/how-much-does-penetration-testing-cost/#:~:text=or%20frameworks%20involved.-,Red%20team%20exercise%20cost,defenses%20and%20incident%20response%20capabilities

Beecroft, N., & Gilmore, T. (2023). *The Advantages of "Hunt Forward" Extend Beyond the Hunt*. BAE Systems | Cyber Security & Intelligence. https://www.baesystems.com/en/digital/feature/the-advantages-of-hunt-forward-extend-beyond-the-hunt

Beretas, C. P. (2023). Analysis of White and Black Hat Hacker Roles, Practices and Techniques, Considering Ethical and Legal Issues, Including Bug Bounty Programs. (Raman) (Lonergan) (Coursera Staff)

Biggerstaff, W. C. (2023, May 10). *The status of Ukraine's "it Army" under the Law of Armed Conflict*. Lieber Institute West Point. https://lieber.westpoint.edu/status-ukraines-it-army law-armed-conflict/

Borges, E. (2024, February 6). *Red Team vs Blue Team in CyberSecurity*. Recorded Future. https://www.recordedfuture.com/threat-intelligence-101/threat-analysis/red-team-vs-blue-team

Cardash , S. L., Cilluffo, F. J., & Ottis, R. (2013). Estonia's Cyber Defence League: A Model for the United States? Taylor & Francis Online, 36(9), 777–787. https://doi.org/https://doi.org/10.1080/1057610X.2013.813273

Carty, D. (2022, August 31). *The Pros and Cons of a Bug Bounty Program.* Applause. https://www.applause.com/blog/the-pros-and-cons-of-a-bug-bounty-program/

Chan, E. (2024, January 22). *Is Pen Testing A Good Career? Unveiling The Reality Behind the Screen*. GadgetMates. https://gadgetmates.com/is-pen-testing-a-good-career-unveiling-the-reality-behind-the-screen

Chng, S., Lu, H., Kumar, A., Yau, D. (2022, March). *Hacker types, motivations, and strategies: A Comprehensive Framework.* Computers in Human Behavior Reports, Volume 5. https://www.sciencedirect.com/science/article/pii/S245195882200001X

Clarke, A. (2021, June 21). *How Often Does the National Guard Respond to Cyberattacks?*. Third Way. https://www.thirdway.org/graphic/how-often-does-the-national-guard-respond-to-cyberattacks

Cole, N. (2022, October 2). *What is red teaming? is it worth doing?*. Network Assured. https://networkassured.com/security/what-is-red-teaming/

Collier, J. (2020, May 21). *Cyber Reserves Are Not A Silver Bullet*. War on the Rocks. https://warontherocks.com/2020/05/cyber-reserves-are-not-a-silver-bullet/

Colorado National Guard Public Affairs (2021, Nov. 1). *Colorado National Guard cyber team assists state during election.* Sixteenth Air Force (Air Forces Cyber). https://www.16af.af.mil/Newsroom/Article/2828707/colorado-national-guard-cyber-team-assists-state-during-election/

Costigliola, F. (2023, January 27). *Kennan's Warning on Ukraine*. Foreign Affairs. https://foreignaffairs.com/ukraine/george-kennan-warning-on-ukraine

Coverage-Based Penetration Testing vs. Depth-Based. (6 Apr, 2021). Packetlabs. https://www.packetlabs.net/posts/coverage-based-penetration-testing/

Critical Infrastructure Sectors. Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Cyber National Mission Force Public Affairs. (2023, June 29). *CYBERCOM's "Under Advisement" to increase private sector partnerships, industry data-sharing in 2023*. U.S. Cyber Command. https://www.cybercom.mil/Media/News/Article/3444464/cybercoms-under-advisement-to-increase-private-sector-partnerships-industry-dat/

Das, R. (2018, August 30). *How are penetration teams structured?*. Infosec. https://infosecinstitute.com/resources/penetration-testing/how-are-penetration-teams-structured/

DDS runs Bug Bounties for the Department of Defense. Hack The Pentagon. (n.d.-a). https://www.hackthepentagon.mil/

Digby, A. (2023, June 7). *How Often Should You Penetration Test?*. Informer. https://informer.io/resources/how-often-should-you-penetration-test

Dugas, M. (2022, February 11). *Cyberspace Multiplier: Enhancing Domestic Cyberspace Resiliency with the National Guard*. N.Y.U. Journal of Legislation & Public Policy. https://nyujlpp.org/quorum/dugas-cyberspace-multiplier/

EEAS Press Team. (2022, December 2). *Ukraine: EU sets up a cyber lab for the Ukrainian Armed Forces*. EEAS. https://www.eeas.europa.eu/eeas/ukraine-eu-sets-cyber-lab-ukrainian-armed-forces_en

EPAM Anywhere Editorial Team. (2024, March 20). *Red Team vs Blue Team in Cybersecurity: Key Roles & Responsibilities*. EPAM Anywhere. https://anywhere.epam.com/en/blog/red-team-vs-blue-team

Evenden, D. (2020, January 2). *Red Teaming @ 10000 Feet*. LinkedIn. https://www.linkedin.com/pulse/red-teaming-10000-feet-david-evenden#:~:text=One%20of%20the%20first%20steps,time%20restraints%20on%20the%20team.

Fabian, E. (2023, July 11). *300 cyberwarfare reservists say they won't volunteer for duty, ...* The Times of Israel. https://www.timesofisrael.com/300-cyberwarfare-reservists-say-they-wont-volunteer-for-duty-as-overhaul-advanced/

Find a Pentesting Provider That Uses the MITRE ATT&CK Framework. Packetlabs. (2024, January 8). https://www.packetlabs.net/posts/find-a-pentesting-provider-that-uses-the-mitreframework/#:~:text=This%20MITRE%20ATT%26CK%20framework%20is,%2C%20analysis%2C%20and%20response%20capabilities.

Fortra. (n.d.). *Red Team*. Fortra. https://www.coresecurity.com/penetration-testing/red-team

Freed, B. (2019, May 15). *What Colorado learned from treating a cyberattack like a disaster*. StateScoop. https://statescoop.com/what-colorado-learned-from-treating-a-cyberattack-like-a-disaster/

Freed, B. (2019b, November 25). *Louisiana issues another emergency declaration over Ransomware*. StateScoop. https://statescoop.com/louisiana-issues-another-emergency-declaration-over-ransomware/

Freed, B. (2021, June 22). *States called National Guard for cyber help at least 41 times since 2018*. StateScoop. https://statescoop.com/states-cybersecurity-national-guard/

Gaia, J., Ramamurthy, B., Sanders, G. L., Sanders, S. P., Upadhyaya, S., Wang, X., & Yoo, C. W. (2020). Psychological Profiling of Hacking Potential. HCSS.

https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/45104877-011f-40d5- 8168-912d83e631e1/content

Garland, I. (2023, May 23). *Cybersecurity job market insights: Analyzing trends and statistics (2021-2023)*. Comparitech. https://www.comparitech.com/blog/information-security/cybersecurity-job-statistics/

General Officer Management Office. (n.d.). *Lieutenant General William J. Hartman (USA)*. https://www.gomo.army.mil/public/Biography/usa-10378/williamj-hartman

Graham, E. (2024, January 19). *Pentagon's cyber red teams get clearer roles, governance*. Nextgov.com. https://www.nextgov.com/cybersecurity/2024/01/pentagons-cyber-red-teams-get-clearer-roles-governance/393481/

Greig, J. (2023, February 24). *Oakland says 311, business license systems still down, but National Guard is helping*. The Record from Recorded Future News. https://therecord.media/oakland-ransomware-systems-still-down-national-guard

Griffiths, Olivia. (2019, February 11). *A British Cyber Defence League?* The Changing Character of War Centre. www.ccw.ox.ac.uk/blog/2015/11/26/a-british-cyber-defence-league.

Grimes, R. (2016, December 6). *Why it's so hard to prosecute cyber criminals.* CSO Online. https://www.csoonline.com/article/559099/why-its-so-hard-to-prosecute-cyber criminals.html

Goncharenko, Oleksiy (2023, February 22). *In War, Ukraine's Parliament Asserts Its Democratic Role*. Just Security. https://www.justsecurity.org/85162/in-war-ukraines-parliament-asserts-its-democratic-role/

"Hack DHS" Program Successfully Concludes First Bug Bounty Program. U.S. Department of Homeland Security. (2022, April 22). https://www.dhs.gov/news/2022/04/22/hack-dhs-program-successfully-concludes-first-bug-bounty-program

Hack the Pentagon. HackerOne. (2024). https://www.hackerone.com/hack-the-pentagon

Hacktivism - A Cyberattack? Meaning, Types, and More. Fortinet. (2024). https://www.fortinet.com/resources/cyberglossary/what-is-hacktivism

Harper, J. (2023, December 15). *New DDS bug bounty to include rapid response capability*. CyberScoop. https://defensescoop.com/2023/12/15/dod-bug-bounty-rapid-response/

Hughes, A. Sgt. 1st C. W. (2022, December 28). *Guard Saved Lives, Property, Responding to 2022 Disasters*. National Guard. https://www.nationalguard.mil/News/Article/3255837/guard-saved-lives-property-responding-to-2022-disasters/

IBM. (n.d.). *What is cyber resilience?*. IBM. https://www.ibm.com/topics/cyber-resilience

Infosec. (2023). *Penetration Tester Career – IT Security Jobs*. https://www.infosecinstitute.com/resources/penetration-testing/penetration-tester-career-security-jobs/

International Group of Experts. (2017). Rule 86 - Participation generally. In *Tallinn Manual 2.0 On The International Law Applicable to Cyber Operations* (pp. 401–401). Cambridge University Press.

International Group of Experts. (2017). Rule 93 – Distinction. In *Tallinn Manual 2.0 On The International Law Applicable to Cyber Operations* (pp. 420-422). Cambridge University Press.

ITU. (2024). *Estonia ranks fifth in the global cybersecurity index*. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Estonia-ranks-fifth-in-the-global-cybersecurity-index.aspx

Karagiannopoulous, V. (2024, October 25). *Ukraine's IT Army is a world first: Here's why it is an important part of the war*. The Conversation. https://theconversation.com/ukraines-it-army-is-a-world-first-heres-why-it-is-an-important-part-of-the-war-212745

Kaushik, A. (2023, December 6). *Ukraine's cyber defence: Insights on private sector contributions since the Russian invasion*. GLOBSEC. https://www.globsec.org/what-we-do/publications/ukraines-cyber-defence-insights-private-sector-contributions-russian

Keary, T. (2023, September 26). *5 Lessons From the Ukraine IT Army's Cyber Operations Against Russia*. Techopedia. https://www.techopedia.com/4-lessons-from-the-ukraine-it-armys-cyber-operations-against-russia

Kirichenko, D. (2023, November 27). *Ukraine's Volunteer IT Army Confronts Tech, Legal Challenges*. CEPA. https://cepa.org/article/ukraine-volunteer-it-army-confronts-tech-legal-challenges/

Kotkin, S. (2016, April 18). *Russia's Perpetual Geopolitics*. Foreign Affairs. https://www.foreignaffairs.com/articles/ukraine/2016-04-18/russias-perpetual-geopolitics

Kozub, S. (2017, February 8). *After cracking the US military, Hackerone gets $40 million in funding*. The Verge. https://www.theverge.com/2017/2/8/14534738/hackerone-bounty-40-million-funding-us-army-vulnerabilities

Krasznay, C. (2024, January 3). *Bridging The Gap: Private Sector's Vital Role In Military Cyber Defense*. White Hat IT Security. https://whitehat.eu/bridging-the-gap-private-sectors-vital-role-in-military-cyber-defense/

Kuik, S. (2023, February 6). *RIA: The number of cyber attacks in 2022 was a hundred times higher than during the April Unrest*. RIA. https://ria.ee/en/news/ria-number-cyber-attacks-2022-was-hundred-times-higher-during-april-unrest

LaDue, Capt. J. (2024, February 14). *Guard Vice Chief Emphasizes Cyber Readiness During Maine Visit*. www.army.mil. https://www.army.mil/article/273740/guard_vice_chief_emphasizes_cyber_readiness_during_maine_visit

Lim, Wei Chieh (2017, August 10). *Hack the Air Force Bug Bounty Program Yields 207 Vulnerabilities*. CPO Magazine. https://www.cpomagazine.com/cyber-security/hack-air-force-bug-bounty-program-yields-207-vulnerabilities/

Mearsheimer, J. J. (2024, August 18). *Why the Ukraine Crisis Is the West's Fault*. Foreign Affairs. https://www.foreignaffairs.com/articles/russia-fsu/2014-08-18/why-ukraine-crisis-west-s-fault

Munive, J. (2016). *RETHINKING THEORIES OF CHANGE IN DDR PROGRAMS*. Danish Institute for International Studies. http://www.jstor.org/stable/resrep13264

NATO. (2023, April 21). *NATO Allies and Partners take part in world's largest cyber defence exercise*. https://www.nato.int/cps/en/natohq/news_214144.htm

NATO Allied Command Transformation. (2023, December 12). *Exercise Crossed Swords Tests Allied Cyber Operations*. NATO. https://www.act.nato.int/article/exercise-crossed-swords-tests-allied-cyber-operations

NGB Public Affairs. (2022, August). *National Guard Cyber Defense Team*. National Guard Bureau. https://www.nationalguard.mil/Portals/31/Resources/Fact Sheets/Cyber Defense Team 2022.pdf

Nieberg, P. (2023, September 28). *"Hunt Forward" cyber teams have deployed to 24 countries, including Ukraine*. Task & Purpose. https://taskandpurpose.com/news/cyber-command-security-huntforward/#:~:text=Known%20as%20%E2%80%9CHunt%20Forward%E2%80%9D%20teams,harm%20from%20any%20possible%20attacks

National Security and Defense Council of Ukraine (NSDC). (2020, November 16). *The NCCC completes the first stage of implementing the "Bug Bounty Pilot Project" for critical infrastructure entities*. https://www.rnbo.gov.ua/en/Diialnist/4742.html?PRINT

Oh, L. (2019). *Exploring Policy Conditions for Cyber Deterrence: A Case Study of Estonia*. Cornell International Affairs Review, 12(2), 121–158. https://doi.org/10.37513/ciar.v12i2.516

O’Neill, P. (2017, February 3). *Dark net markets moving to adopt bug bounty programs.* CyberScoop. https://cyberscoop.com/dark-net-markets-bug-bounty-programs/

Pell, S. (2022, December 1). *Private-sector cyber defense in armed conflict*. Lawfare. https://www.lawfaremedia.org/article/private-sector-cyber-defense-armed-conflict

Penetration Testing. (2024). Syopsys. https://www.synopsys.com/glossary/what-is-penetration-testing.html

Plamann, J. (n.d.). *Continued National Guard Integration in the Total Cyber Mission & Training: Fiscal Year 2025 Fact Sheet*. NGAUS. https://www.ngaus.org/sites/default/files/2024-03/Cyber%20Fact%20Sheet%20FY25.pdf

Pomerleau, M. (2023, June 8). *US Cyber Command conducts "hunt forward" mission in Latin America for first time, official says*. DefenseScoop. https://defensescoop.com/2023/06/08/us-cyber-command-conducts-hunt-forward-mission-in-latin-america-for-first-time-official-says/

Private Sector Collaboration Pathway. USAID. (n.d.). https://www.usaid.gov/work-usaid/private-sector-engagement/private-sector-collaboration-pathway

Razmi, R., & Barlow, E. (2023, October). *Red and Blue Cyber Teams – A Tactical Arena!*. SecurityHQ. https://www.securityhq.com/blog/red-and-blue-cyber-teams-a-tactical-arena/

Red teaming: Everything You Need To Know. CovertSwarm. (n.d.). https://www.covertswarm.com/post/red-team-assessment#:~:text=Benefits%20of%20red%20teaming&text=Improving%20security%20posture%3A%20by%20addressing,to%20develop%20effective%20response%20plans

Red Team Operations and Adversary Emulation. (2022, August 29). National Initiative for Cybersecurity Careers and Studies (NICCS). https://niccs.cisa.gov/education-training/catalog/sans-institute/red-team-operations-and-adversary-emulation

Render-Katolik, A. (2023, August 15). *The IT Army of Ukraine: Strategic technologies blog*. CSIS. https://www.csis.org/blogs/strategic-technologies-blog/it-army ukraine#:~:text=The%20IT%20Army%20of%20Ukraine%20has%20mobilized%20thou a nds%20of%20volunteers,Russia’s%202022%20invasion%20of%20Ukraine

RIA. (2023, November 11). *Major Cyber Exercise Tested Country’s Cyber Reserve*. ERR. https://news.err.ee/1609162126/major-cyber-exercise-tested-country-s-cyber-reserve

Rijnetu, I. (2024, March 20). *100+ essential penetration testing statistics [2023 edition]*. Pentest Tools. https://pentest-tools.com/blog/penetration-testing-statistics

Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2018, April). An Introduction to Cyber Peacekeeping. https://dora.dmu.ac.uk/server/api/core/bitstreams/d9850454-bc55-4b87- 9223-2a91479c327a/content

Rockeman, O. (2022, April 1). *Hackers' Path Eased as 600,000 Cybersecurity Jobs Sit Empty (1)*. Bloomberg Law. https://news.bloomberglaw.com/privacy-and-data-security/hackers-path-is-eased-as-600-000-cybersecurity-jobs-sit-empty

Romagna, M., & Leukfeldt, R. E. (2023). Becoming a hacktivist. Examining the motivations and the processes that prompt an individual to engage in hacktivism. *Journal of Crime and Justice*, 1–19. https://doi.org/10.1080/0735648X.2023.2216189

Rudin, David. "Hackers for Hire Help Companies Find Their Weak Spots | Financial Post." *Financial Post*, 3 Mar. 2023, financialpost.com/cybersecurity/hackers-help-companies- find-weak-spots.

Shore, J. (2022, April 11). Don't underestimate Ukraine's volunteer hackers. Foreign Policy. https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers it- army/

Siripurapu, A., & Berman, N. (2024, April 3). *What Does the U.S. National Guard Do?*. Council on Foreign Relations. https://www.cfr.org/backgrounder/what-does-us-national-guard-do#:~:text=The%20National%20Guard%20is%20an,domestic%20crises%20and%20overseas%20conflicts

Sivesind, C. (2023, July 7). *"Under Advisement" Bridges Gap Between US Government, Private Industry*. Cybersecurity Conferences & News. https://www.secureworld.io/industry-news/under-advisement-doubling-staff

Soesanto, S. (2022, June). *CYBERDEFENSE report - ETH Z*. Center for Strategic Studies (CSS), ETH Zurich . https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for securities-studies/pdfs/Cyber-Reports-2022-08-One-Two-or-Two-Hundred-Internets.pdf

Sorensen, M., Remy, J., Kjettrup N., Mahmoud, V., & Pedersen, M. J., (2018). *An Approach to Detect and Prevent Cybercrime in Large Complex Networks*. International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Glasgow, UK. doi: 10.1109/CyberSecPODS.2018.8560687.

Soucy, Sgt. 1st C. J. (2019, November 15). *Guard cyber teams key asset in cyber defense*. Texas Military Department. https://tmd.texas.gov/guard-cyber-teams-key-asset-in-cyber-defense

State Service of Special Communications and Information Protection of Ukraine (SSSCIP). (2022, April 4). *In Ukraine, the use of Bug Bounty has been standardized. What is it - and how will it help?*. State Service of Special Communications And Information Protection of Ukraine. https://cip.gov.ua/en/news/v-ukrayini-uzakonili-bug-bounty-sho-ce-i-yak-dopomozhe

Talaber, A., Mosher, D., & Keating, E. G. (2020, June). *Costs of Creating a Space National Guard*. Congressional Budget Office. https://www.cbo.gov/publication/56384

Temple-Raston, D. (2023, June 30). *Exclusive: Inside an American hunt forward operation in Ukraine*. The World. https://theworld.org/stories/2023-06-30/exclusive-inside-american-hunt-forward-operation-ukraine

Temple-Raston, D., & Powers, S. (2023, October 20). *Exclusive: How a defend-forward operation gave Ukraine's SBU an edge over Russia*. The Record from Recorded Future News. https://therecord.media/illia-vitiuk-interview-ukraine-sbu-defend-forward

Temple-Raston, D., & Powers, S. (2022, August 29). *Inside the IT Army of Ukraine, "A Hub for Digital Resistance."* The Record from Recorded Future News. https://therecord.media/inside-the-it-army-of-ukraine-a-hub-for-digital-resistance

Temple-Raston, D., Powers, S., & Atoniuk, D. (2023, October 18). *Exclusive: Ukraine says Joint Mission with US derailed Moscow's cyberattacks*. The Record from Recorded Future News. https://therecord.media/ukraine-hunt-forward-teams-us-cyber-command

Texas Military Department. (2023, September 14). *State Partnership Program Brings Together Chile and Texas Guard for Cyber Training*. https://tmd.texas.gov/state-partnership-program-brings-together-chile-and-texas-guard-for-cyber-training

The Government approved the Procedure for Bug Bounty in Ukraine. Better Regulation Delivery Office. (2023, May 17). https://brdo.com.ua/en/news/uryad-zatverdyv-poryadok-provedennya-bug-bounty-v-ukrayini/

The New Voice of Ukraine. (2023, December 6). *A snapshot of Ukraine's Armed Forces* . https://english.nv.ua/nation/a-snapshot-of-ukraine-s-armed-forces-50374392.html

U.S. Army Cyber Command (2022, September 1). *Hack The Army*. https://www.arcyber.army.mil/Resources/Fact-Sheets/Article/3106335/hack-the-army/#:~:text=The%20bug%20bounties%20aim%20to,find%20vulnerabilities%20in%20those%20sites.

U.S. Bureau of Labor Statistics. (2023, September 6). *Information security analysts : Occupational Outlook Handbook*. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#:~:text=About%2016%2C800%20openings%20for%20information,force%2C%20such%20as%20to%20retire

U.S. Cyber Command Public Affairs. (2022, April 22). *Guard, Reserve Component Summit exemplifies "Cyber Is a Team Sport."* U.S. Cyber Command.

https://www.cybercom.mil/Media/News/Article/3008313/guard-reserve-component-summit-exemplifies-cyber-is-a-team-sport/

U.S. Cyber Command PAO. (2022, October 25). *Cyber 101 - Defend Forward and Persistent Engagement*. U.S. Cyber Command. https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/

U.S. Cyber Command Public Affairs. (2022, November 15). *Cyber 101: Hunt Forward Operations*. 960th Cyberspace Wing. https://www.960cyber.afrc.af.mil/News/Article-Display/Article/3219164/cyber-101-hunt-forward-operations/

U.S. Cyber Command Public Affairs. (2022, December 30). *U.S. Cyber Command 2022 Year in Review*. U.S. Cyber Command. https://www.cybercom.mil/Media/News/Article/3256645/us-cyber-command-2022-year-in-review/

U.S. Cyber Command. (2020, December 3). *Estonia, U.S. Conduct Joint Defensive Cyber Operation*. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/2434474/estonia-us-conduct-joint-defensive-cyber-operation/

US Federal. (2024). HackerOne. https://www.hackerone.com/solutions/united-states-federal

U.S. Government Bug Bounty Programs Here to Stay Under Trump Administration. (2017, February 14). Infosecurity Magazine. https://www.infosecurity-magazine.com/news/rsac-us-government-bug-bounty/

U.S. Government Publishing Office. (2022, April 27). *Civilian Cybersecurity Reserve Act*. Senate report 117-97 - Civilian Cybersecurity Reserve Act. https://www.govinfo.gov/content/pkg/CRPT-117srpt97/html/CRPT-117srpt97.htm

United States Department of Defense. (2023). *Defense Budget Overview*. Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer. https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2023/FY2023_Budget_Request_Overview_Book.pdf

Vergun, D. (2022, December 3). *Partnering With Ukraine on Cybersecurity Paid Off, Leaders Say*. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/3235376/partnering-with-ukraine-on-cybersecurity-paid-off-leaders-say/

What is a phishing attack? Cloudfare. (2024). https://www.cloudflare.com/learning/access-management/phishing-attack/

What is a zero-day exploit?. IBM. (n.d.). https://www.ibm.com/topics/zero-day

What is DDOS Attack?. Fortinet. (2024). https://www.fortinet.com/resources/cyberglossary/ddos-attack#:~:text=DDoS%20Attack%20means%20%22Distributed%20Denial,connected%20online%20services%20and%20sites.

What is Malware?. McAfee. (2024). https://www.mcafee.com/en-us/antivirus/malware.html

What is penetration testing?. Cloudfare (2024). https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/

What is Social Engineering. Imperva. (2024). https://www.imperva.com/learn/application-security/social-engineering-attack/

Whyte, C. (2024, March 20). *5 ways private organizations can lead public-private cybersecurity partnerships*. CSO Online. https://www.csoonline.com/article/2066511/5-ways-private-organizations-can-lead-public-private-cybersecurity-partnerships.html

ZipRecruiter. (2024). *Red Team Penetration Tester Salary*. ZipRecruiter. https://www.ziprecruiter.com/Salaries/Red-Team-Penetration-Tester-Salary#:~:text=As%20of%20Mar%2015%2C%202024,States%20is%20%24119%2C895%20a%20year.