2022 PRAGUE

28 - 30 September, 2022 / Prague, Czech Republic

THE THREAT IS STRONGER THAN THE EXECUTION: REALITIES OF HACKTIVISM IN THE 2020S

Blake Djavaherian

Mandiant, USA

Blake.Djavaherian@Mandiant.com

ABSTRACT

Authentic hacktivist threat actors – while frequently overlooked by researchers and overshadowed by state-nexus operations utilizing hacktivist personas for cover – have continued to proliferate globally. Yet such actors still tend to be plagued by the same phenomena that have historically stymied others in the hacktivism landscape from either achieving operational maturity or fulfilling demonstrable objectives at levels most often associated with advanced persistent threat (APT) or well-organized cybercriminal groups. These stumbling blocks include weak hierarchical structures, limited technical knowledge across members, and pervasive behavioural immaturity.

As a result, the vast majority of hacktivists to emerge in recent years have pursued inconsistent objectives, experience short lifespans, and fail to cause the grandiose impacts they loudly promise. This overall trend has manifested in the swarm-like nature of campaigns conducted by modern hacktivist 'collectives' – including Anonymous – whose operations are often as over-hyped as they are short-lived. These campaigns are occasionally assisted by leak publishing entities such as whistleblowing groups (e.g. Distributed Denial of Secrets) or by external organizational efforts (e.g. the Ukrainian government's recruitment for an IT Army of Ukraine).

These trends are not necessarily the rule: at least one hacktivist group, the Belarusian Cyber Partisans, has exhibited advanced organizational and operational security skills above and beyond its counterparts. Since August 2020, the Cyber Partisans have conducted high-profile, and even impactful, information operations and disruptive attacks against the Belarusian government in protest against the policies and continued administration of the country's executive, Aleksander Lukashenko. While that group has targeted Belarusian government entities in 2022 in an effort to degrade Russian military logistics associated with the latter's invasion of Ukraine, its precise origins remain a subject of some debate.

This paper explores the state of contemporary hacktivism, beginning with the formation and activities of loose collectives, before continuing on to describe the nature, interactions and operations of hacktivist groups within regional hacktivist ecosystems. It then examines the Cyber Partisans through the lens of being an outlier among authentic hacktivist groups, leading into a concluding analysis on the broader implications of the development of advanced hacktivist entities operating in opposition to, or support of, national governments.

INTRODUCTION

In 2022, the spectrum of cyber threat intelligence (CTI) research continues to centre around the best-resourced, most technically brilliant, and most impactful activity available for both novel research and audience-grabbing public disclosure. Despite the enduring value of such research in connection to state-nexus and ecrime-oriented threat actors, additional groups that fail to reach widely accepted metrics of sophistication may not receive the requisite attention they deserve, to the detriment of the field overall. Hacktivists are one such example.

For the purposes of this paper, hacktivist threat actors are defined as entities whose use of offensive cyber capabilities hinges primarily around personal and ideological motivations, rather than the demands of a sponsoring state or in the pursuit of financial gain. Said motivations may range from political ideology to self-realized nationalistic and theological associations, to even the simple desire for attention and development of clout. These examples are by no means mutually exclusive, and the very nature of hacktivist groups enables them – as well as their individual members, acting either on behalf of the overall group or in a personal capacity – to be spurred on by a fluid set of underlying factors.

This fluidity may bleed into motivations that overlap with other threat actor categories, such as a state-nexus group's devoted patriotic support for a national government or a criminal enterprise's pursuit of financial gain. The line between a purely hacktivist group and these auxiliary motivations – due, perhaps, to a hacktivist's activity during a geopolitical crisis or extortionary activity tangential to ideologically motivated activities – may at times be nebulous and very difficult to measure. Entities like KelvinSecTeam, whose claims have simultaneously blended schemes to sell data for profit, commitments to ideological causes [1], and intentions to cause problems for little apparent reason other than to garner attention [2], highlight this ambiguity. As did LulzSec, an offshoot from genuine hacktivist forums who in the end was found primarily to be motivated by little more than the desire for attention [3], and the Syrian Electronic Army, whose ostensibly independent support for Syrian President Bashar Al Assad was complicated by his explicit approval [4]. While challenging to gauge objectively, the often-blurred line between hacktivists and other threats highlights the multifaceted, dynamic nature of hacktivists' capabilities, targeting and goals.

CONTEMPORARY HACKTIVIST GROUP CHARACTERISTICS

Hacktivists and the communities they form tend to follow patterns that both encourage the emergence of new groups and yet constrain the credibility, operational effectiveness and longevity that these entities typically achieve. These patterns include:

- Loose group structures prone to weak overall cohesion.

- Comparatively unsophisticated technical capability development based on rapid incorporation of immediately available – often open-source – resources.
- Pervasive immaturity and non-professionalism.

Together, these factors offer a foundational point of view for understanding contemporary trends in hacktivist behaviour. Additionally, these can serve as a basis toward developing an appreciation for hacktivists whose formations improve upon or entirely disregard these trends – highlighting the exceptional nature of hacktivist groups that possess long-term perspectives with regard to ideological vision, tradecraft investment and public relations.

At the same time, these characteristics also illustrate the difficulty of assessing attribution in relation to activity conducted by hacktivist threat actors, whose allegiances may appear simultaneously personal, group-oriented, and associated with a collective identity – as opposed to clearly delegated from a single point of origin or motivation.

Structure

Hacktivists – much like traditional activists – in general prefer to coalesce and act in groups, which inherently offer greater access to resources, collaborative opportunities, and amplification for political messaging. These benefits more often than not incentivize aspiring hacktivists to associate themselves at least informally with established groups and collectives. This is not to say that individual hacktivists have not in the past conducted impactful operations: the pseudonymously named Phineas Fisher's activity between 2014 and 2019 resulted in instances of major corporate, government and individual defamation [5], and encouragement for others to follow suit [6]. Much more often, however, individual hacktivists lack the discipline or skill set to carry through to completion more than foundational offensive cyber operations, if not simply exaggeration or outright falsified claims on social media for attention and artificial clout.

Authentic hacktivists rarely develop robust, formalized hierarchies or enact standard operational processes. Unlike state-operated targeted intrusion threat actors, hacktivist groups are not guided by bureaucratic organizational requirements consistent with the demands of a government institution. Nor are hacktivists faced with the same economic and operational security requirements as well-organized cybercriminal groups, whose outsize sources of illicit funding and ambitions for enterprise-level scaling often result in obedience to hierarchy and professionalism [7].

Instead, grassroots hacktivist entities typically consist of individuals who decide to associate and conduct activity with one another based on one or more shared beliefs. This provides for a high level of flexibility that lends itself to fluid organizational ties unique to hacktivism. Hacktivist entities are as a result able to collaborate, combine, dissolve, and otherwise reformulate with greater ease than many other threat actors.

While the decentralization of authority involved in this approach might attract like-minded individuals with at least the idea of common goals, the same advantage more often produces entities made up of loosely affiliated, poorly resourced, and less professional individuals stumbling in the direction of a hoped for – but rarely well-defined – outcome. Most authentic hacktivist entities fitting this description belong to at least one of two categories:

1. Loose collectives of disparate, largely autonomous individuals and subgroups dispersed regionally or globally.
2. Small, comparatively cohesive working groups centring around a smaller pool of individuals, potentially accompanied by close followings whose broader participation is generally minimal.

These categories are not entirely comprehensive nor mutually exclusive; for example, an individual hacktivist belonging to a named group associated with a broader collective may claim activity conducted separately from both. However, given the preponderance of individual hacktivists' movement between and within entities meeting these definitions, they serve as useful points of reference toward understanding the interactions of hacktivist entities.

Collectives

Collectives represent a common avenue for hacktivists to project their personal ideologies without being forced into even the modest hierarchical demands of a defined group. Collectives feature individuals loosely bound by name and sometimes a level of direct coordination between affiliates. In spite of their common ties, affiliates otherwise remain primarily independent from one another in terms of planning and acting on mission scopes related to the cyclical whims of the collective's ideology. The Anonymous collective, a global movement broadly based on tenets advancing personal freedom and opposing corruption, has remained the most widespread and influential over time [8].

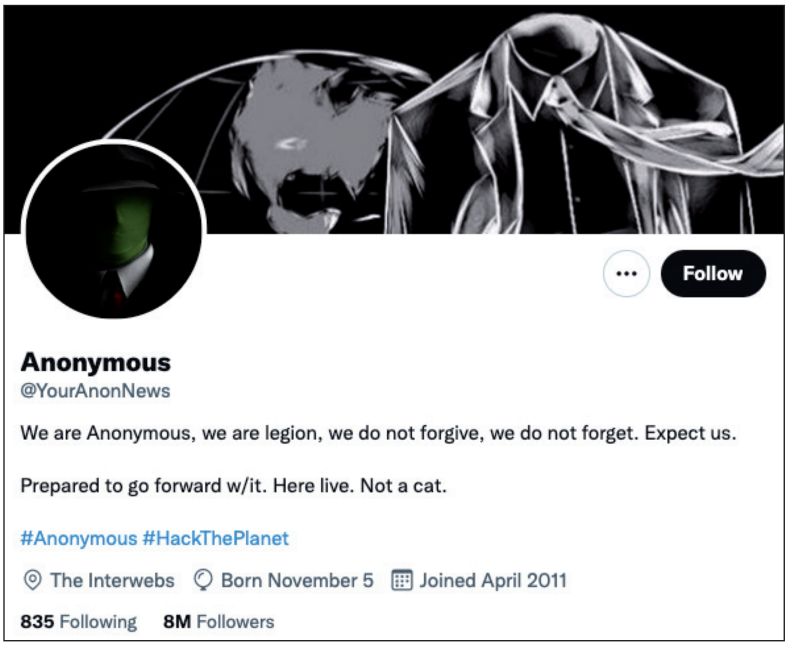
Collective decentralization feeds on popular momentum during times of domestic political or geopolitical drama. These periods of heightened tension frequently lead hacktivists to use mostly uncoordinated swarm tactics to target entities associated with the origin of the controversy. These campaigns often manifest quickly and are labelled following a standard nomenclature represented by the format: `#Op[Name]`. Some such sets of activity are scheduled to take place on an annual basis, like previous iterations of `#OpIsrael`, which has more recently failed to stick to premeditated scheduling [9]. Campaigns may also form ad hoc in response to domestic government upheaval, such as the coordination of activity targeting Nicaraguan President Daniel Ortega's government in `#OpNicaragua` in 2020 and again in 2021 for pandemic denials and fraudulent electoral practices, respectively (see Figure 1) [10, 11, 12].

Figure 1: Imagery associated with the Anonymous campaign #OpNicaragua.

Contentious government policies, such as those surrounding women's reproductive rights, can also spark hacktivist campaigns. `#OperationJane`, for example, came about in response to challenges to US abortion rights [13]. Hacktivists also target private organizations seen as complicit in malicious activity, such as in the 2021 breach of the controversial web hosting provider Epik in `#OperationEpikFail` [14].

Structurally, the implications for hacktivist activity as a result of collectivization are mixed. On the one hand, collectives broadly allow for an inclusive array of participants. This in turn enables faster tactical decision-making, ease of mobilization, and a larger pool of individuals potentially possessing technical skills and resources upon which the group may draw. In addition, collectives' decentralized nature allows for individual hacktivists or small groups to signal ideology and intentions at low cost, thus removing a major obstacle for many hacktivists to overcome. Established members, such as Anonymous's Lorian Synaro, often leverage substantial personal followings to unilaterally attract attention to the collective as a whole without being bogged down by the institutional realities of a formalized group structure [15]. Moreover, members without a developed brand are able to rely on the collective's reputation to increase the scope of their potential audience, allowing them to focus greater attention on technical development and operations.

However, these benefits in operational flexibility and amplification come with inherent negative consequences. These include disorganized and potentially incoherent messaging, unvetted associations with bad actors who can cause reputational damage, and a broad lack of institutional support for members to develop and refine technical skills. These factors result in an overall diminished likelihood of generating tangible impacts. They also risk generating unintended blowback against broader portions of the collective than those responsible for a subset of poorly calculated activity. The pro-Russia hacktivist entity Killnet, whose loose collection of subgroups and affiliates has orchestrated numerous distributed denial-of-service (DDoS) attacks against targets within Ukraine and its allies, has on several occasions displayed moments of internal tension, with affiliates that have conducted activity antithetical to the collective's overall goals [16]. For example, on 15 May 2022, the primary Killnet *Telegram* channel deflected blame for a thwarted DDoS attack targeting the semi-finals of the Eurovision Song Contest, which it attributed to a 'disobedient' affiliate [17, 18].



Anonymous
@YourAnonNews

We are Anonymous, we are legion, we do not forgive, we do not forget. Expect us.

Prepared to go forward w/it. Here live. Not a cat.

#Anonymous #HackThePlanet

The Interwebs Born November 5 Joined April 2011

835 Following **8M** Followers

Figure 2: Prominent Twitter profile associated with the Anonymous collective.

As with Killnet, collectives often feature numerous subdivisions, branches, and tangential copycats that represent their respective ideologies on a more granular basis. Anonymous itself is divided into regional foci whose volumes of activity cycle dramatically in tandem with geopolitical developments specific to those regions. Even further, individual operators, close supporters, and even self-identifying spokespeople – some of whom have amassed very large followings on social media (see Figure 2) – provide additional insights into current ideological lines upheld by at least some, if not a majority or nearly all members of such collectives.

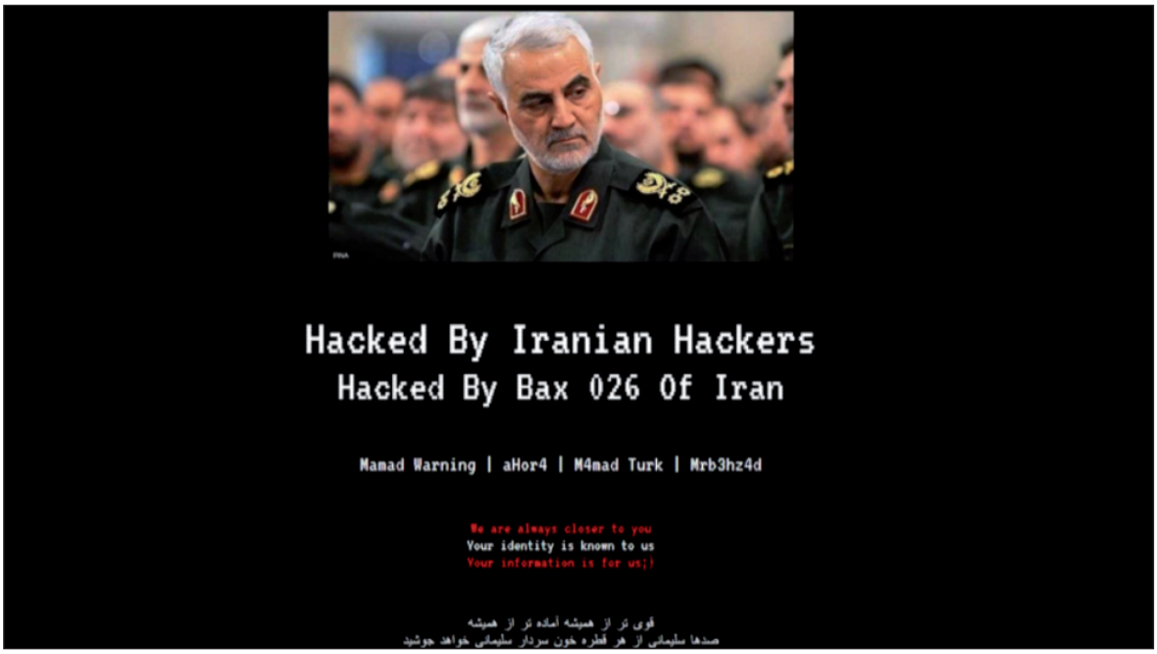
Working groups

Some hacktivists conduct activity through the formation of small, better defined working groups with a comparatively higher level of cohesion. These offer opportunities to generate greater impacts through the combination of individuals' respective skill sets and reputations. Within this pattern, the strength and duration of associations between individual hacktivists vary widely. For example, the Egyptian Cyber Horus Group, which targeted Ethiopian entities in June 2020 in protest against that country's construction of an upriver dam on the Nile [19], provided a singular group name and represented a unitary set of apparent motivations [20]. This lies in contrast to entities whose members leave behind personal aliases or commit other expressions of individual identity within group operations.

Hacktivists who have already developed individual reputations may view collaboration as an exercise in fleeting cooperation only meant to serve a short-term goal. Such partnerships may or may not operate under a joint pseudonym, depending on the longevity of the coupling. Sporadic collaborations between geographically disparate individuals exemplify this point, such as the explicitly stated partnership between Iranian hacktivist group Bax026 and the Brazilian hacker VandaTheGod [21, 22]. This partnership resulted in several website defacements before VandaTheGod's arrest by Brazilian authorities in March 2021 [23].

In some cases, hacktivist groups will make use of consolidated social media channels to distribute claims and market their activities to external followers. In some instances, these groups may also attempt to involve and potentially recruit from their base of followers, occasionally staging professional-looking websites to attract attention and appear more legitimate. The Turkish hacktivist group Ayyildiz Tim, for example, maintains a domain detailing its motivations through an about page, a blog, and a forum, among other online materials engineered to engage its audience [24]. A group's reputation for credibility and the size of its social media presence can also serve toward determining its standing with other hacktivist groups, with implications for recruitment efforts.

Due in part to the necessity for shared styles of communication – including common language use and cultural cues – between individuals active in such groups, their proliferation tends to foster regional hacktivist ecosystems. Groups within such ecosystems have opportunities to both collaborate and compete with one another. Ecosystems may at times develop into pseudo-collectives of their own, as hacktivists begin to associate themselves both with their respective groups and with the broader collection of hacktivists operating parallel to them. Iranian hacktivists in particular often conduct website defacements featuring the header 'Hacked by Iranian Hackers' in even larger font than the name of their group or individual aliases (see Figure 3).



Hacked By Iranian Hackers
Hacked By Bax 026 Of Iran

Mamad Warning | aHor4 | M4mad Turk | Mrb3hz4d

We are always closer to you
Your identity is known to us
Your information is for us;)

قوی تر از همیشه آماده تر از همیشه
صدها سلیمانی از هر قطره خون سردار سلیمانی خواهد جوشید

Figure 3: Website defacement of a Carmel, IN, government domain by Iranian hacktivists in 2020.

As in Iran, nationalism represents a frequent common denominator between regional hacktivist working groups. Following the killing of Iranian general Qassem Soleimani in January 2020, multiple Iranian hacktivist groups – including Bax026 [25], Unidentified_TM [26], Liosion Team [27], ICTUS Team [28] and Shield Iran [29], among others – employed overlapping imagery of Soleimani in subsequent website defacements of Western entities [30], some of which were conducted jointly by individual hacktivists belonging to different Iranian groups [31].

While the Iranian hacktivist ecosystem is associated broadly with long-standing patriotic sentiments, others may coalesce around shared cultural, theological, or other mutual similarities. In Turkey, for example, hacktivists similarly conduct nationalistic activity [32], though these are supplemented by religiously motivated operations in support of Muslims abroad [33]. Ecosystems can at times become indistinguishable from regional subgroups of collectives, such as in several Latin American countries, where many hacktivists simply identify with their corresponding regional affiliate of Anonymous [34, 35]. Most importantly, the nature and variety of regionally associated ecosystems reflect how geography, culture and identity intersect with the fluidity of hacktivist bodies.

Capabilities

Hacktivists have historically relied on rudimentary, readily available, and rapidly deployable offensive cyber capabilities. The primary tactics, techniques, and procedures (TTPs) associated with hacktivists most often serve operations meant to deny service, deface digital resources, or leak stolen data. In nearly all cases, these tactics are employed to cause a combination of reputational harm and operational cost to victim entities. While these broader strategies have remained intact across observed hacktivist activity into the 2020s, contemporary hacktivists continue to improve and expand upon historical tactics, including most notably through the incorporation of ransomware.

Denials of service, defacements and data leaks

Denial of service operations offer hacktivists a quick method to disrupt target infrastructure without the need for significant reconnaissance or other target-specific preparations. DDoS activity against a given target is also easy to claim and its impacts are readily verifiable (i.e. the ease of checking whether a website is offline at a given time). This immediate upside and low resource cost make these attacks a preferred tactic for many hacktivists.

Similar to denials of service, website defacements permit hacktivists to directly disrupt the routine operations of a target organization through manipulation of public-facing network infrastructure. Unlike denial of service activity, website defacements add the additional opportunity for hacktivists to co-opt that infrastructure for their own use, providing a forum for them to credibly claim and divulge motivations behind their activity. Moreover, in spite of timely remediations of successful defacements, online archives such as *Zone-H* allow hacktivists to freely upload evidence of their own exploits for future reference [36].

Data leaks, despite being more indirect in their disruptive capacity than denials of service are arguably more damaging to a victim, and are another common hacktivist tactic. Leaking operations are by far most effective when threat actors are able to demonstrate the veracity of their activity; however, hacktivists frequently do recycle leaks they or other hacktivists have previously conducted – or even allege that information available in open sources constitutes a leak – while claiming the information re-shared is novel.

Issues with the credibility of certain leaks can be mitigated by third-party leak publishers, such as *Distributed Denial of Secrets* (*DDoSecrets*). Prior to posting data leaks, *DDoSecrets* vets such information to a considerable extent so as to ensure that information posted to its platform is in fact novel, notable, and does not contain potentially harmful personally identifiable information (PII) [37].

Incorporation of ransomware into hacktivist operations

Ransomware has more recently begun to serve as a major tool for certain hacktivist groups to significantly increase the disruptiveness and costliness of their intrusions. In the past, hacktivists were limited in the extent they could leverage a compromised network in the hope of encountering sensitive files to manually delete or exfiltrate. With growing access to ransomware tools that were once out of reach, however, hacktivists can much more reliably and effectively disable target systems than they were previously capable of doing.

Ideologically motivated ransomware attacks are becoming increasingly common. A particularly notable case occurred in March 2021, in which hacktivists deployed a new ransomware family – dubbed Sarbloh – to Indian victims in connection to national protests led by farmers opposing a sudden overhaul of agricultural subsidy laws [38]. Instead of demanding a ransom in exchange for restored system access, however, Sarbloh encrypted victim computers with a note denying a decryption key until the farmers' demands were met [39]. More recently, the ostensibly altruistic GoodWill ransomware promises a decryption key for encrypted files only after the victim completes a specifically requested 'good deed' and publishes video evidence to social media [40].

Unconventional uses of ransomware present substantial risk, especially in light of hacktivists' inconsistent and unprofessional operational styles. Namely, the lack of a mature operational culture on the part of hacktivists reduces the chance that the victim of an ideologically motivated ransomware attack will be able to negotiate successfully for a decryption key. It remains unclear if GoodWill successfully encrypted any victims, though if it had, there is similarly no evidence indicating the group responsible would genuinely monitor for or care to accept attempts by victims to follow its instructions [41].

In other cases in which the primary objective of the hacktivist group is purely to disrupt the target rather than to modify their behaviour, providing a decryption key at any point may prove antithetical to the operation's goals. In recently observed hacktivist operations reliant on ransomware – primarily those conducted in relation to the ongoing war in Ukraine, elaborated in a subsequent section – hacktivists have combined traditional ransomware tactics with support for their respective causes. This includes leveraging the promise of decryption keys to negotiate for the redirection of ransomware-extorted funds to relevant charities, the liberation of political prisoners, and even the wartime withdrawal of military forces [42].

THE BELARUSIAN CYBER PARTISANS AND EVIDENCE OF EVOLUTION IN HACKTIVIST ORGANIZATION IN THE 2020s

Contemporary hacktivism has not yet undergone a widespread evolution in terms of the incentives, structures and capabilities described above. In spite of this, one hacktivist group breaks with several historical precedents: the Belarusian Cyber Partisans. Since late 2020, the Cyber Partisans have effectively organized, developed technical capabilities, and managed public relations in a professional manner above and beyond the typical expectations of nearly all other hacktivist groups in their pursuit of regime change against Belarusian President Alexander Lukashenko.

Background

On 9 August 2020, Lukashenko – the incumbent since 1994 – fraudulently claimed to have won over 80 per cent of the vote in Belarus's presidential elections [43]. These results were marred by a combination of the obvious inflation of overall voter turnout, results almost impossibly skewed in Lukashenko's favour, and underlying public tensions stemming from national economic woes as well as domestic mismanagement of the COVID-19 pandemic [44, 45].

In the following weeks, hundreds of thousands of Belarusians filled Minsk's and other Belarusian city centres to protest against the fraudulent election as Lukashenko's exiled opposition rival, Sviatlana Tsikhanouskaya, declared herself the victor [46]. This mass movement of people resulted in international attention as well as domestic crackdowns on foreign journalists, the brutal deployment of internal security forces, and thousands of arrests of mostly peaceful protesters [47]. The Lukashenko regime's violent response was quickly followed by Western condemnation and economic sanctions [48].

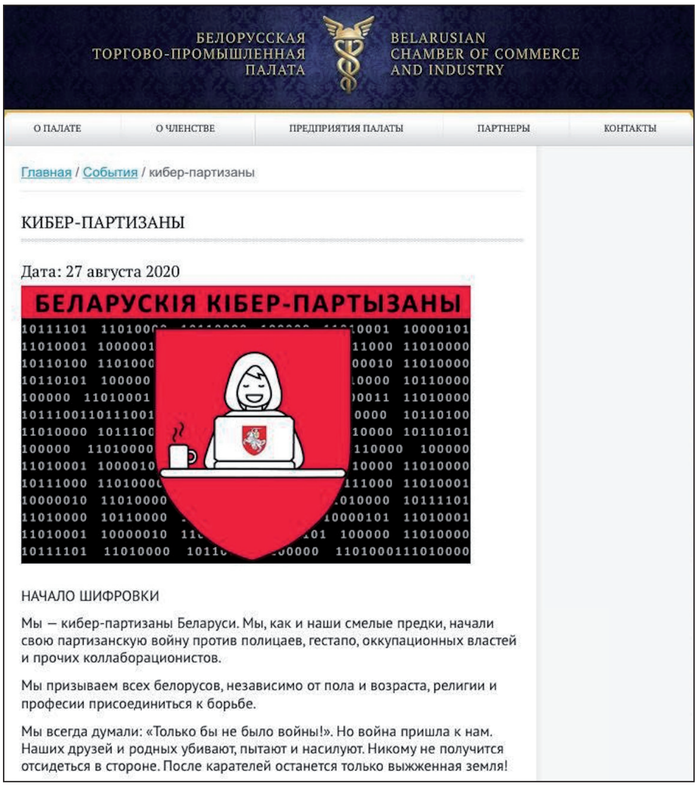
While this was not the first time fraudulent Belarusian presidential elections had resulted in major public backlash – as had happened on multiple other occasions, including the 2006 and 2010 elections that resulted in Western economic sanctions lasting until 2016 – ubiquitous public access to digital technologies likely increased the effectiveness, visibility and security of participants within the country's most recent protest movement. This includes the use of tools enabling secure communications and coordination of groups on a major scale, as well as virtual private networks (VPNs) and other tools enabling secure, anonymous access to the Internet [49]. These tools served a critical role in allowing protesters to overcome the state's Internet blockade and content restrictions [50].

Emergence

Amid this sequence of domestic political upheaval, the Cyber Partisans formed from a collection of information technology professionals intent on directing their technical skills against the Belarusian government [51]. Initially, the group primarily claimed modestly disruptive activity targeting agencies of the Belarusian government. Its earliest known operation took place on 5 September 2020 with the defacement of multiple government web pages, including that of the state Chamber of Commerce and Industry's website [52]. The group replaced the page's contents with their own logo alongside a letter advocating for government resistance (see Figure 4), serving as the first known introduction to the group and its associated imagery. The Cyber Partisans soon followed this activity with multiple additional website defacements, which the group maintained into October 2020 [53].

While likely effective for seeking an initial audience for the group's social media channels [54, 55], this initial wave of website defacements was for the most part displaced by hack-and-leak operations orchestrated to dox, embarrass, and implicate in nefarious activity members of the Belarusian government. On 9 September 2020, the group's earliest disclosure of stolen data featured a government web page defaced with a link to an archive of payment records and residential addresses purportedly belonging to members of the country's State Security Committee (KGB) [56, 57]. Since that time, subsequent Cyber Partisans victims have included various government entities, including organizations associated with the president, law enforcement and investigative bodies, members of the national judiciary, and even affluent individuals perceived to have relationships with the Lukashenko government [51].

Leaks have consisted variously of internal network data, PII – such as troves of passport records, including those of Lukashenko's son – and other forms of sensitive information, including phone conversations implicating the Belarusian


БЕЛОРУССКАЯ ТОРГОВО-ПРОМЫШЛЕННАЯ ПАЛАТА
BELARUSIAN CHAMBER OF COMMERCE AND INDUSTRY
О ПАЛАТЕ
О ЧЛЕНСТВЕ
ПРЕДПРИЯТИЯ ПАЛАТЫ
ПАРТНЕРЫ
КОНТАКТЫ
БЕЛАРУСКІЯ КІБЕР-ПАРТЫЗАНЫ

Главная / События / кибер-партизаны

КИБЕР-ПАРТИЗАНЫ

Дата: 27 августа 2020

НАЧАЛО ШИФРОВКИ

Мы – кибер-партизаны Беларуси. Мы, как и наши смелые предки, начали свою партизанскую войну против полицаев, гестапо, оккупационных властей и прочих коллаборационистов.

Мы призываем всех белорусов, независимо от пола и возраста, религии и професии присоединиться к борьбе.

Мы всегда думали: «Только бы не было войны!». Но война пришла к нам. Наших друзей и родных убивают, пытают и насилуют. Никому не получится отсидеться в стороне. После карателей останется только выжженная земля!

Figure 4: August 2020 defacement of Belarusian Chamber of Commerce and Industry website.

government in wire-tapping schemes against foreign government missions within Belarus [58]. Since their earliest operations, the Cyber Partisans have often timed activity to coincide with real-world events; to this end, the group has arbitrarily imposed deadlines on organizations viewed as tangentially complicit in the activities of the Belarusian government. On 26 October 2020, for example, they conducted a DDoS attack that brought down the website of the National Bank of Belarus for several hours in response to the organization's refusal to join nationwide strikes [59]. Later, on 14 January 2021, the Cyber Partisans released a collection of Belarusian officials' PII as a result of another set of ignored demands for law enforcement accountability made to the Central Apparatus of the Investigative Committee [60].

Although the group has staged several such deadlines, they are also reactionary to developing events. This includes their 23 May 2021 compromise and sabotage of the network of the Academy of Public Administration under the President of the Republic of Belarus – for which the group cited as their root motivation Belarus's interception of a commercial flight to arrest an opposition journalist earlier that same day [61].

Collaborations and public relations

The Cyber Partisans have not entirely focused operational impacts around leaks or directly disruptive operations targeting the Belarusian government. In addition to these goals, the group has built and maintained positive relationships with independent protesters. On multiple occasions, the Cyber Partisans have announced they would develop digital infrastructure and tools to assist other resistance groups and anti-government protesters. On 25 October 2020, for example, the group promised to stage proxy servers to facilitate secure communications between protesters [62]. Later, in mid-2021, the group announced it would release an encrypted SMS application for a similar purpose, foreshadowing the group's release of a security-oriented, bespoke version of *Telegram*. This software – dubbed 'Partisan Telegram' – was designed specifically for the Partisans' audience as well as protesters 'in other countries with authoritarian regimes' [63].

The Cyber Partisans are not the sole Belarus-based activist group to have established strong resistance against the government during this period. The group exists as part of a broader alliance with two other groups – the Flying Storks and the People's Self-Defence Squads (PSS) – which identifies as the Suprativ movement [64]. According to the alliance's website, their overarching objective is to overthrow the Lukashenko regime and establish robust democracy in Belarus. Within their partnership, the Cyber Partisans primarily offer offensive cyber expertise, the Flying Storks the conduct of physical sabotage against Belarusian infrastructure, and the PSS educational resources to assist individuals during mass protests [51]. The Cyber Partisans have additionally benefited from a partnership with the dissident organization of former Belarusian government officials ByPol, which provides clarification and tips on potential targets of activity for Suprativ's member groups [65].

Figure 5: The logos of the Suprativ alliance (left to right: Cyber Partisans, Flying Storks, PSS).

The Cyber Partisans have also collaborated with journalists and researchers at multiple points during this time. In August 2021, the Cyber Partisans worked with the Western-funded, Russian-language media outlet Current Time TV to leak large volumes of COVID-19 mortality data contradictory to the government's official tally of deaths due to the virus, drastically undercutting the Lukashenko regime's narrative on the issue [66]. Later, in November 2021, a collaborative effort with the investigative outlet *Bellingcat* led the Cyber Partisans to provide prosecutorial documents associated with the trial of alleged Russian private military contractors allegedly targeted in a convoluted sting operation orchestrated by Ukrainian security services [67]. It remains unclear to what extent the Cyber Partisans have collaborated directly with these investigative outlets, beyond the provision of broad sets of data from victim entities; however, the group's willingness to directly assist third parties who have the resources and initiative to sort, analyse, and publicly communicate findings based on the group's leaking activity provides a distinctly strong avenue for the hacktivists to make their work actionable.

Group tradecraft

Scant details regarding the Cyber Partisans' specific operational tradecraft have become public over time, much of which can be attributed to the nature of their targeting – which has yet to deviate from direct operations against Belarusian state entities. In January 2021, industry reporting revealed that the Partisans themselves shared a third-party incident report in relation to a compromise they had orchestrated at the presidential academy in March 2021 [68]. According to details within the report – which the Cyber Partisans hinted at in a video published in November 2021 [69] – the group's offensive capabilities largely draw from open-source tools, including Nmap, Mimikatz, and publicly available code for exploits such as BlueKeep (CVE-2019-0708). Additionally, the Cyber Partisans employed living-off-the-land tactics to perform lateral movement and establish persistence. This included the use of remote desktop protocol (RDP) to move across the victim network, TCP port forwarding to establish consistent external connection to Cyber Partisan-controlled infrastructure, and legitimate credentials. The incident response notes the hacktivists leveraged their access to wipe data from both active and backup systems, consistent with the group's claims.

The Cyber Partisans indicated that the incident response report only demonstrated a subset of the tools in use by the group, and declined to share additional, potentially custom, tools deployed in that incident as well as in other intrusions. This is notable given the fact that the group has since employed tools oriented specifically toward destructive ends – especially ransomware, which has played a key role in operations since late 2021.

In addition, the Cyber Partisans have made prior references to so-called 'cyber bombs' left on victim networks post-compromise, potentially referring to webshells or similar tools left behind to maintain persistence for future exploitation. The group has also repeatedly alleged the development of a custom malware tool mysteriously called X-App [70]. The group claims that in the future, at the time of a so-called 'Moment-X', the group and its partners will attempt to paralyse government institutions using computer network attack (CNA) operations involving X-App, as well as concurrent support activity for physical sabotage and protest operations carried out by affiliated groups (see Figure 6).

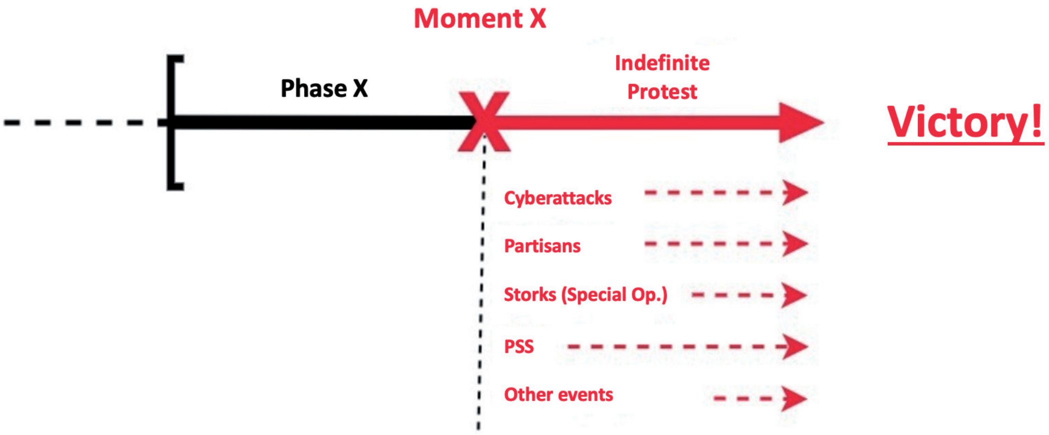


Figure 6: Rough translation of Moment-X graphic provided by the Cyber Partisans.

The Cyber Partisans are unique in their public relations strategy in that they filter information regarding motivations, tactics, and operational claims through an individual spokesperson, the currently New York-based Yulyana Shemetovets. Thanks to the consistent stream of interviews and statements provided by Shemetovets in her campaigning to maintain positive publicity for the group, some organizational details about the secretive Partisans have come to light. In terms of size and structure, Shemetovets has previously revealed that the Partisans consisted of about 15 members in late 2021, with the intention of doubling in early 2022; as of mid-2022, an interview with a purported member of the group puts the current total number closer to 60 [71]. Of these members, Shemetovets insists that only a very small minority conduct offensive operations and have access to the full spectrum of data the group steals; meanwhile, the rest of the group provides support roles, and includes 'developers, testers, and data analysts' [72]. In keeping with the group's commitment to transparency, the Cyber Partisans have even offered breakdowns of their use of third-party donations [73].

As far as hierarchy is concerned, Shemetovets has insisted the Cyber Partisans largely operate as a cohesive unit in which decisions are made by council. While it remains unclear whether every member holds equal sway over the group's strategic or tactical goals, these comments suggest the group at least partially democratizes internal decision making, in contrast to most hacktivist entities' decentralized decision-making processes. Combined with the establishment of an organizational structure with well-defined roles and diversity of institutionally necessary responsibilities, these tenets of the Cyber Partisans' group structure show the strength of the organization they have successfully developed since their emergence.

Campaigns

The Cyber Partisans have announced two long-term campaigns during their existence so far. The first, announced under the name Operation Heat (alternatively: Operation Heat Wave, Operation Scorching Heat) in July 2021, regularized the group's leaking activity throughout the second half of that year into the end of November 2021. Leaks were released to the group's social media channels in numbered dossiers called 'Weather Reports', providing a comparatively standard format through which leaks could be distributed. In total, the Cyber Partisans published 24 Weather Reports as part of Operation Heat.

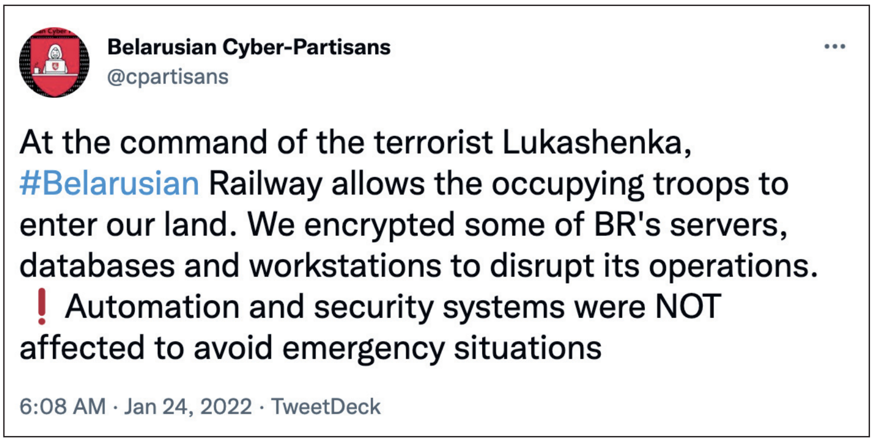
While Operation Heat was still ongoing, the group announced the start of a new campaign, Operation Hellfire (alternatively: Operation Inferno) on 17 November 2021. Whereas Operation Heat emphasized leaks, the new campaign centred around direct sabotage of government systems, with claims summarized in a new series of Weather Reports. Importantly, this campaign featured the group's first expansive use of ransomware to make demands on Belarusian state entities.

Operation Hellfire began with the defacement and encryption of systems belonging to the presidential academy [74]. The second of these Weather Reports, in which the Cyber Partisans claimed to have encrypted and exfiltrated large portions of the network of a state-owned potash fertilizer producer, arrived on 28 November 2021 [75]. Subsequently, in early December 2021, the campaign claimed victim a state-affiliated railway car manufacturing entity, and offered decryption in exchange for the release of several political prisoners of the group's choosing [76].

Onset of conflict in Ukraine

Following Russia's invasion of Ukraine on 24 February 2022, the conflict in Ukraine has proven a tenuous proving ground for the resilience of the Cyber Partisans in their continuation of Operation Hellfire. The transition to wartime hacktivism has also become a venue for the group to demonstrate the strength of its cohesion and technical capabilities.

Preceding the war, the Belarusian government complied extensively with Russia's belligerent geopolitical goals. An especially contentious aspect of this international partnership was Belarus's allowance for Russian armed forces to amass along Belarus's border with Ukraine in the beginning of 2022 [77]. The Cyber Partisans quickly took note and, as part of its ongoing campaign, claimed to compromise and encrypt systems belonging to the state-owned entity Belarusian Railway to disrupt Russian movements (see Figure 7) [78].



Belarusian Cyber-Partisans
@cpartisans

At the command of the terrorist Lukashenka, #Belarusian Railway allows the occupying troops to enter our land. We encrypted some of BR's servers, databases and workstations to disrupt its operations.
❗ Automation and security systems were NOT affected to avoid emergency situations

6:08 AM · Jan 24, 2022 · TweetDeck

Figure 7: Initial public claims targeting Belarusian Railway.

These efforts continued over the following months, allegedly leading to persistent disruptions of train scheduling [79]. In addition, while the Cyber Partisans claimed their cyber operations – in combination with physical sabotage of Belarusian rail lines by the Flying Storks – halted formal Russian military logistics through Belarus, the group further claimed in March 2022 that the Russian military had reconvened and moved to use unmarked freight trains to transport equipment and ammunition into Ukraine [80].

Standing out from the crowd

In addition to the Cyber Partisans, multiple established and newcomer groups have pledged allegiance either to the side of Ukraine and its allies or to Russia. Prominent pro-Ukraine hacktivists active during this time include various affiliates of Anonymous, who have contributed significant dumps of data to *DDoSecrets* under the campaign name `#OpRussia` [81]. In addition, the war has attracted more unconventional hacktivists, such as the pro-Ukraine group Squad303, whose online resources provide a method for individuals outside of the conflict to send anti-war messages to Russian citizens [82].

While more closely affiliated than Anonymous, none of these groups have yet to demonstrate the longevity or long-term vision characteristic of the Cyber Partisans; in addition, the at-times competitive and petty nature of much of their activity reflects the continued influence of ego at play in many hacktivists' personal conduct. In spite of this, the Ukrainian government recognized the potential for this outpouring of hacktivist attention devoted to the conflict early on, with government officials soliciting their assistance as early as 25 February 2022 [83]. This effort culminated in the development of the so-called IT Army of Ukraine. Since that time, accounts associated with the IT Army of Ukraine have claimed various operations against Russian targets designated as entities of interest by the group's administrators. Despite these ostensible successes, the IT Army of Ukraine has also been plagued by various issues surrounding staffing and ambiguity of group leadership as well as accountability standards [84], leading some Western officials to discourage individuals from taking part in the group's activities [85].

One group founded during this time, Network Battalion 65 (NB65), has conducted repeated deployments of a modified version of the Conti ransomware against exclusively Russian targets, using the malware as a method to extort organizations and attempt to generate cash to donate to charities associated with the Ukrainian war effort [42]. NB65 has become prolific as a result, with numerous claims of ransomware and leaks against victims spanning Russian managed service providers [86], financial entities [87], and logistics companies [88], among others during this period.

Despite the two groups' common TTPs – principally, the employment of ransomware as a method of ideological coercion – there remain key differences between NB65 and the Cyber Partisans. In contrast to the Cyber Partisans, NB65 has exhibited a more opportunistic target scope, impacting public and private entities alike [89]. Additionally, they have not demonstrated the same level of operational planning and capability for data distribution, with no signs that NB65 has the built-in institutional support functions of the Cyber Partisans. *DDoSecrets* has at least supplemented the group's ability to make use of data stolen in the course of its activity; however, NB65's directed opportunism and intrinsic need to outsource functions such as the sorting of data dumps reflects the lesser capabilities of this group as well as others active during this time in comparison to the Cyber Partisans.

CONCLUSION

Across the contemporary hacktivist landscape, no single factor has come about to significantly disrupt the ways hacktivists coalesce to form associations or conduct activity. Rather, the pattern of change has been incremental, with a range of variables – including the broadening willingness of personnel with technical expertise to take part in hacktivist activity, the necessity of improved information security surrounding protest movements, and the increasing availability of effective offensive security resources – driving this evolution. No hacktivist group illustrates these changes as much as the Cyber Partisans. The group's emergence in September 2020 and rapid development into a legitimate threat to its target scope is exceptional in a field in which structural shortcomings typically hamstring groups with similar aspirations.

In particular, the incorporation of ransomware into the Cyber Partisans' arsenal mirrors tactical innovations by other threat actors, such as in cybercriminal extortion campaigns [90] and Iranian state-nexus lock-and-leak activity [91, 92]. These parallels shed light on the variety of ways that these increasingly disruptive and accessible capabilities can be appropriated to achieve distinct objectives. The use of ransomware by the Cyber Partisans to directly demand political concessions reflects just one such implementation, while the variety of hacktivist uses for ransomware already observed goes to show that the trend as a whole is likely subject to further innovations.

Despite the systemic restraints holding back hacktivists' potential to execute on par with the threats they make, though, the successes of the Cyber Partisans since their emergence demonstrate the increasing potential for upstart hacktivist groups to form and tie themselves to specific causes. This trend potentially represents a harbinger for a future of hacktivism in which increasingly lowered barriers to entry provide for more and more avenues for groups such as the Cyber Partisans to come about and pursue tangible action in cyberspace.

The Cyber Partisans, for all their professionalism, technical expertise, and institutional development, maintain the singular goal of seeing Alexander Lukashenko and his government removed from power. While the group may in some form persist past such a point, the completion of this task should imply the dissolution of the Cyber Partisans as they currently exist. The reality of single-issue hacktivism is that groups formed to address a problem should inherently not be designed to outlive it. This is not the case for all hacktivist groups, of course, as many causes – such as nationalism and ideology – may be ambiguous and impossible to ever fully overcome. However, for hacktivists such as the Cyber Partisans, whose cause is indelibly finite, the fleeting, democratic nature of their associations may represent more of a feature rather than a flaw, representing the transient demands that spur the phenomenon of authentic hacktivism in the first place.

REFERENCES

[1] @Ksecureteamlab. Twitter. March 2022. https://twitter.com/Ksecureteamlab/status/1505715248472465411.

[2] Allstate Identity Protection. The evolving threat landscape: nation states, third-party attacks, and the dark web. https://blog.infoarmor.com/security-professionals/threat-landscape-nation-states-third-party-attacks-dark-web.

[3] Arthur, C. LulzSec: what they did, who they were and how they were caught. The Guardian. May 2013. https://www.theguardian.com/technology/2013/may/16/lulzsec-hacking-fbi-jail.

[4] Fowler, S. Who is the Syrian Electronic Army? BBC News. April 2013. https://www.bbc.com/news/world-middle-east-22287326.

[5] Phineas Fisher. Vice. https://www.vice.com/en/topic/phineas-fisher?page=1.

[6] Fisher, P. HackBack - A DIY Guide For Those Without The Patience To Wait For Whistleblowers. Packet Storm. April 2017. https://packetstormsecurity.com/files/142322/HackBack-A-DIY-Guide-For-Those-Without-The-Patience-To-Wait-For-Whistleblowers.html.

[7] https[:]//www.justice[.]gov/opa/press-release/file/1445241/download.

[8] Huddleston, T. Jr. What is Anonymous? How the infamous ‘hacktivist’ group went from 4chan trolling to launching cyberattacks on Russia. CNBC. https://www.cnbc.com/2022/03/25/what-is-anonymous-the-group-went-from-4chan-to-cyberattacks-on-russia.html.

[9] Balduzzi, M.; Flores. R., Gu, L.; Maggi, F. A Deep Dive into Defacement: How Geopolitical Events Trigger Web Attacks. Trend Micro. https://documents.trendmicro.com/assets/white_papers/wp-a-deep-dive-into-defacement.pdf.

[10] Vida, M. Anonymous group hack reveals hidden government data about COVID-19 cases in Nicaragua. Global Voices Advox. August 2020. https://advox.globalvoices.org/2020/08/31/anonymous-group-hack-reveals-hidden-government-data-about-covid-19-cases-in-nicaragua/.

[11] Flores, C. Anonymous comienza a atacar sitios web del régimen Ortega-Murillo. La Mesa Redonda. April 2020. https://www.lamesaredonda.net/anonymous-comienza-a-atacar-sitios-web-del-regimen-ortega-murillo/.

[12] Mendoza Y.; Kitroeff, N. Nicaragua Descends Into Autocratic Rule as Ortega Crushes Dissent. New York Times. November 2021. https://www.nytimes.com/2021/11/07/world/americas/nicaragua-election-ortega.html.

[13] Stuart, T. A Pro-Choice Hacking Team Defaced the Texas GOP Website. So We DM’d Them. Rolling Stone. October 2021. https://www.rollingstone.com/politics/politics-features/meet-the-woman-led-hacking-team-that-defaced-the-texas-gop-website-1238782/.

[14] Thalen, M. New leak of Epik data exposes company’s entire server. Daily Dot. September 2021. https://www.dailydot.com/debug/anonymous-new-epik-leak/.

[15] iAfrikan News. Lorian Synaro of Anonymous explains the motive behind #OpSudan and #OpZimbabwe. TNW. January 2019. https://thenextweb.com/news/lorian-synaro-of-anonymous-explains-the-motive-behind-opsudan-and-opzimbabwe.

[16] Vedere Labs. Killnet. Analysis of Attacks from a Prominent Pro-Russian Hacktivist Group. Forescout. https://www.forescout.com/resources/analysis-of-killnet-report/.

[17] Askew, J. Eurovision 2022: Russian hackers targeted contest, say Italian police. Euronews. May 2022. https://www.euronews.com/culture/2022/05/16/eurovision-2022-russian-hackers-targeted-contest-say-italian-police.

[18] Killnet Channel. Telegram. https://t.me/killnet_channel.

[19] Berta, N. ‘Cyber Horus’ hacking group mounts cyberattack on 37,000 computers in connection with Grand Ethiopian Renaissance Dam. Addis Zeybe. June 2021. https://addiszeybe.com/featured/currentaffairs/technology/cyber-horus-hacking-group-mounts-cyberattack-on-37-000-computers-in-connection-with-grand-ethiopian-renaissance-dam.

[20] Mahmoud, R. Egypt hackers attack Ethiopian sites as Nile dam talks falter. Al-Monitor. June 2020. https://www.al-monitor.com/originals/2020/06/egypt-cyber-attack-ethiopia-nile-dam-dispute.html.

[21] Bax 026 Of Iran. Twitter. March 2021. https://web.archive.org/web/20210323222920/https://twitter.com/Bax026/status/1374488410824445952.

[22] Check Point Research. Bringing VandaTheGod down to Earth: Exposing the person behind a 7-year hacktivism campaign. May 2020. https://research.checkpoint.com/2020/vandathegod/.

[23] Palma, G., Netto, W. PF prende hackers suspeitos de participação no vazamento de dados de 223 milhões de brasileiros. Globo.com. March 2021. https://g1.globo.com/economia/tecnologia/noticia/2021/03/19/policia-federal-deflagra-operacao-contra-divulgacao-e-comercializacao-de-dados-pessoais-de-brasileiros.ghtml.

[24] https[:]//ayyildiz[.]org/.

[25] Treadstone 71. Wisconsin County Hacks Bax026 of Iran. The Cyber Shafarat. August 2021. https://cybershafarat.com/2021/08/01/w8sconsin-county-hacks-bax026-of-iran/.

[26] Unidentified TEAM. Telegram. https://t.me/Unidentified_TM.

[27] Gatlan, S. FBI Releases Alert on Iranian Hackers' Defacement Techniques. Bleeping Computer. January 2020. https://www.bleepingcomputer.com/news/security/fbi-releases-alert-on-iranian-hackers-defacement-techniques/.

[28] TAPESH DIGITAL SECURITY TEAM IRAN. Telegram. https://t.me/ICTUS_TM.

[29] Cox, J. Iranian Hackers Claim Defacement of Texas Government and Alabama Veterans Websites. Vice. January 2020. https://www.vice.com/en/article/m7qa83/iranian-hackers-deface-texas-government-website.

[30] Current Publishing. City of Carmel shuts down website after discovering it had been hacked. September 2020. https://www.youarecurrent.com/2020/09/18/city-of-carmel-shuts-down-website-after-discovering-it-had-been-hacked/.

[31] United States Department of Justice. Two Alleged Hackers Charged with Defacing Websites Following Killing of Qasem Soleimani. September 2020. https://www.justice.gov/opa/pr/two-alleged-hackers-charged-defacing-websites-following-killing-qasem-soleimani.

[32] Gutman, Y. Battle for Supremacy | Hacktivists from Turkey and Greece Exchange Virtual Blows. Sentinel One. January 2020. https://www.sentinelone.com/blog/battle-for-supremacy-hacktivists-from-turkey-and-greece-exchange-virtual-blows/.

[33] Salas-Rodriguez, I. DON TRUMPED 'Donald Trump's website HACKED' by 'Turkish and Muslim Hacktivist' warning 'do not be like those who forgot Allah'. The Sun. October 2021. https://www.thesun.co.uk/news/16457966/donald-trumps-website-hacked-turkish-muslim-hacktivist/.

[34] Aguirre A., F. Anonymous hackea sitio web de Carabineros y exponen datos de todos los efectivos del país. La Tercera. October 2019. https://www.latercera.com/que-pasa/noticia/anonymous-hackea-sitio-web-carabineros-exponen-datos-todos-los-efectivos-del-pais/878328/.

[35] Rapoza, K. Brazil's President Bolsonaro Latest Victim Of Anonymous Hackers. Forbes. June 2020. https://www.forbes.com/sites/kenrapoza/2020/06/02/brazils-president-bolsonaro-latest-victim-of-anonymous-hackers/?sh=5c70a12a6607.

[36] Zone-H. http://www.zone-h.org/archive.

[37] Distributed Denial of Secrets. https://ddosecrets.com.

[38] Mashal, M.; Schmall, E.; Goldman, R. What Prompted the Farm Protests in India. New York Times. January 2021. https://www.nytimes.com/2021/01/27/world/asia/india-farmer-protest.html.

[39] Sandapolla, T. Sarbloh: a new ransomware that does not demand money. Quick Heal blog. https://blogs.quickheal.com/activists-turn-hacktivists-new-ransomware-that-does-not-demand-money/.

[40] CloudSEK. GoodWill ransomware forces victims to donate to the poor and provides financial assistance to patients in need. May 2022. https://cloudsek.com/threatintelligence/goodwill-ransomware-forces-victims-to-donate-to-the-poor-and-provides-financial-assistance-to-patients-in-need/.

[41] Boyd, C. Eerie GoodWill ransomware forces victims to publish videos of good deeds on social media. Malwarebytes Labs. May 2022. https://blog.malwarebytes.com/ransomware/2022/05/eerie-goodwill-ransomware-forces-victims-to-publish-videos-of-good-deeds-on-social-media/.

[42] Soesanto, S. Are Hacktivist Data Dumps Helping Ukraine? The National Interest. June 2022. https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/are-hacktivist-data-dumps-helping.

[43] Bilefsky, D.; Higgins, A. Who Is Aleksandr G. Lukashenko? Here's What You Need to Know. New York Times. November 2021. https://www.nytimes.com/2021/11/11/world/who-is-aleksandr-g-lukashenko.html.

[44] Human Rights Defenders for Free Elections. Republic of Belarus. 2020 Presidential Election. Report on Early Voting. 2020. https://spring96.org/files/misc/2020_milestone_early_voting_09.08_en.pdf.

[45] Haltiwanger, J. Europe's last dictator got COVID-19 after telling people they could avoid it by drinking vodka and going to the sauna. Business Insider. June 2020. https://www.businessinsider.com/europe-last-dictator-belarus-lukashenko-covid-19-vodka-sauna-2020-7.

[46] Filkins, D. The Accidental Revolutionary Leading Belarus's Uprising. The New Yorker. December 2021. https://www.newyorker.com/magazine/2021/12/13/the-accidental-revolutionary-leading-belaruss-uprising.

[47] Human Rights Watch. Belarus: Systematic Beatings, Torture of Protesters. September 2020. https://www.hrw.org/news/2020/09/15/belarus-systematic-beatings-torture-protesters.

[48] European Council. Timeline - EU restrictive measures against Belarus. https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-belarus/belarus-timeline/.

[49] Psiphon. Psiphon Guide. https://psiphon.ca/en/psiphon-guide.html.

[50] International Strategic Action Network for Security. BELARUS PROTESTS: INFORMATION CONTROL AND TECHNOLOGICAL CENSORSHIP VS CONNECTED SOCIETIE. NATO Strategic Communications Centre of Excellence. December 2020. https://stratcomcoe.org/cuploads/pfiles/belarus_protests_web_nato_stratcom_coe.pdf.

[51] Suprativ's operations and projects. August 2021. https://telegra.ph/Suprativs-Operations-08-24.

[52] @El_espanola. Twitter. September 2020. https://web.archive.org/web/20200905174557/https://twitter.com/El_espanola/status/1302301204379324416.

[53] @maxwsmeets. Twitter. May 2022. https://twitter.com/maxwsmeets/status/1525108258356498432.

[54] Belarusian Cyber-Partisans. Telegram. https://t.me/cpartisans.

[55] Belarusian Cyber-Partisans. Twitter. https://twitter.com/cpartisans.

[56] @VoicesBelarus. Twitter. September 2020. https://web.archive.org/web/20200909171053/https://twitter.com/VoicesBelarus/status/1303742121917255681.

[57] Soshnikov, A.; Andrejeva, M.; Romaliiska, I.; Owen, E. Seeking Change, Anti-Lukashenka Hackers Seize Senior Belarusian Officials' Personal Data. Current Time. August 2021. https://en.currenttime.tv/a/seeking-change-anti-lukashenka-hackers-seize-senior-belarusian-officials-personal-data-/31392092.html.

[58] Настоящее Время. Opposition hackers got access to the materials of telephone wiretaps of the Ministry of Internal Affairs of Belarus. June 2022. https://www-currenttime-tv.translate.goog/a/belarus-mvd-proslushka/31898037.html?_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=wapp.

[59] Nexta TV. Telegram. October 2020. https://t.me/nexta_tv/7592.

[60] Belarusian Cyber-Partisans. Telegram (archive). November 2020. https://archive.ph/ffukh.

[61] Belarusian Cyber-Partisans. Telegram (archive). https://archive.ph/k1j1N.

[62] @Maxwsmeets. Twitter. May 2022. https://twitter.com/maxwsmeets/status/1525108258356498432.

[63] wrwrabbit / Partisan-Telegram-Android. GitHub. https://github.com/wrwrabbit/Partisan-Telegram-Android.

[64] Manifesto on the establishment of the Belarusian Resistance alliance - Suprativ. August 2021. https://telegra.ph/Supratsiu-Manifesto-08-24.

[65] Howell O'Neil, P. Hackers are trying to topple Belarus's dictator, with help from the inside. MIT Technology Review. August 2021. https://www.technologyreview.com/2021/08/26/1033205/belarus-cyber-partisans-lukashenko-hack-opposition/.

[66] Soshnikov, A. Excess mortality - 32 thousand people. Belarusian authorities repeatedly underestimate statistics during the coronavirus epidemic – leaked data. Настоящее Время. August 2021. https://www.currenttime.tv/a/smertnost-v-belarusi/31401342.html.

[67] Bellingcat Investigation Team. Inside Wagnergate: Ukraine's Brazen Sting Operation to Snare Russian Mercenaries. Bellingcat. November 2021. https://www.bellingcat.com/news/uk-and-europe/2021/11/17/inside-wagnergate-ukraines-brazen-sting-operation-to-snare-russian-mercenaries/.

[68] @BushidoToken, @SteveD3. Hacktivist group shares details related to Belarusian Railways hack. Curated Intelligence. January 2022. https://www.curatedintel.org/2022/01/hacktivist-group-shares-details-related.html.

[69] Cyber-partisans. Cyberattack on Lukasheko's Academy. YouTube. https://www.youtube.com/watch?v=8l4etG0YKKQ.

[70] Cyber-Partisan's victory plan. August 2021. https://telegra.ph/Cyber-Partisans-victory-plan-08-24.

[71] Gallagher, R. Hackers Is Waging Cyberwar on Putin's Supply Lines. Bloomberg. June 2022. https://www.bloomberg.com/news/features/2022-06-15/ukraine-war-attracts-belarusian-hackers-in-fight-vs-putin.

[72] Gostoli, Y. How I became the spokesperson for a secretive Belarusian ‘hacktivist’ group. TRT World. February 2022. https://www.trtworld.com/magazine/how-i-became-the-spokesperson-for-a-secretive-belarusian-hacktivist-group-54617.

[73] @cpartisans. Twitter. March 2022. https://web.archive.org/web/20220311192829/https://twitter.com/cpartisans/status/1502365809250914312.

[74] @cpartisans. Twitter. November 2021. https://web.archive.org/web/20211117222751/https://twitter.com/cpartisans/status/1461098759266488322.

[75] @cpartisans. Twitter. November 2021. https://web.archive.org/web/20211130223912/https://twitter.com/cpartisans/status/1465222960193712129.

[76] @cpartisans. Twitter. December 2021. https://web.archive.org/web/20211210160914/https://twitter.com/cpartisans/status/1469326661426597896.

[77] Toosi, N., Forgey, T. U.S. slams Russian troop moves in Belarus as Ukraine crisis deepens. Politico. January 2022. https://www.politico.com/news/2022/01/18/blinken-europe-ukraine-russia-tensions-527257.

[78] Gallagher, R. A Ragtag Band of Hackers Is Waging Cyberwar on Putin’s Supply Lines. Bloomberg. June 2022. https://www.bloomberg.com/news/features/2022-06-15/ukraine-war-attracts-belarusian-hackers-in-fight-vs-putin.

[79] @cpartisans. Twitter. March 2022. https://web.archive.org/web/20220302142928/https://twitter.com/cpartisans/status/1499028956305149954.

[80] @belzhd_live. Telegram. https://t.me/belzhd_live/1338.

[81] Distributed Denial of Secrets. Category:Russia. https://ddosecrets.com/wiki/Category:Russia.

[82] https://1920.in/.

[83] Burgess, M. Ukraine’s Volunteer ‘IT Army’ Is Hacking in Uncharted Territory. Wired. February 2022. https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/.

[84] NPR. Volunteer hackers form ‘IT Army’ to help Ukraine fight Russia. March 2022. https://www.npr.org/2022/03/27/1089072560/volunteer-hackers-form-it-army-to-help-ukraine-fight-russia.

[85] Milmo, D. Amateur hackers warned against joining Ukraine’s ‘IT army’. The Guardian. March 2022. https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army.

[86] @xxNB65. Twitter. May 2022. https://web.archive.org/web/20220520044133/https://twitter.com/xxNB65/status/1527509603952599048.

[87] @xxNB65. Twitter. May 2022. https://web.archive.org/web/20220504232644/https://twitter.com/xxNB65/status/1521994538423881728.

[88] @xxNB65. Twitter. April 2022. https://web.archive.org/web/20220405223353/https://twitter.com/xxNB65/status/1511472012925050880.

[89] Menn, J. Hacking Russia was off limits. The Ukraine war made it a free-for-all. The Washington Post. May 2022. https://www.washingtonpost.com/technology/2022/05/01/russia-cyber-attacks-hacking/.

[90] Crowdstrike. What Is Cyber Big Game Hunting? March 2022. https://www.crowdstrike.com/cybersecurity-101/cyber-big-game-hunting/#:~:text=Cyber%20big%20game%20hunting%20is,organizations%20or%20high%2Dprofile%20entities.

[91] Cyberwarcon. Their Own Little War: Iran Adopts Disruptive Ransomware. November 2021. https://www.cyberwarcon.com/their-own-little-war.

[92] Starks, T. Ransomware isn’t always about gangs making money. Sometimes it’s about nations manufacturing mayhem. Cyberscoop. January 2022. https://www.cyberscoop.com/disruptive-ransomware-iran-russia-china/.