

Zero Day Nation: The Secret War of Cyber Power

Understanding the New Frontlines of Power in the Cyber Age

By Jeremy Makowski
Cyber Crime and Terrorism Intelligence Expert

July 31, 2025

Disclaimer

This document is made freely available for informational purposes and to support a deeper understanding of the evolving dynamics of power in the cyber age.

Reproduction of any part of this document whether in whole or in part must include proper attribution to the author and a clear reference to the original source.

Any commercial use of the content, in full or in part, is strictly prohibited without the express written consent of the author.

Table of Content

Disclaimer **2**
Table of Content **3**
Introduction **7**
Part I: Understanding the Cyber Sphere **9**
Chapter 1: Origins of Cyberspace **9**
1.1 From ARPANET to Global Internet 9
1.2 Evolution into a Strategic Domain 10
1.3 The Rise of Digital Dependence 11
Chapter 2: Anatomy of the Digital World **12**
2.1 Physical Infrastructure 12
2.2 Network Infrastructure 12
2.3 Access Infrastructure 13
2.4 Web Infrastructure 13
2.5 Application & Protocol Layer 13
2.6 Security Infrastructure 13
Chapter 3: Behavior in the Digital Age **17**
3.1 Human Online Behaviour 17
3.2 Impact on Cyber conflicts 20
Part II: Cyber Warfare: Crime, Conflict, and Control in a Digital World **21**
Chapter 4: Cybercrime Ecosystem and Operations **21**
4.1 Cybercriminal Platforms 21
4.1.1 Forums 22
4.1.2 Automatic Selling Marketplace 26
4.1.3 Underground Markets 28
4.1.4 Encrypted Messaging Applications 30
4.2 Cybercrime Organizational Structure: **31**
4.3 Cybercriminal's Modus Operandi and Operations **34**
4.3.1 Open Source Intelligence 34
4.3.2 Social Engineering 36
4.3.3 Virtual HUMINT 44
4.3.4 Malware and Exploits 46
4.3.5 Network Access and Data Breach 54
4.4 Cybercriminals' Psychology **56**
4.4.1 Motivations 56
4.4.2 Psychological Profiles 57
4.5. Geographical Distribution of Cybercrime **58**
4.5.1. Western Europe and North American Countries 58
4.5.2. Eastern European Countries 60
4.5.3. Middle East and African Countries 62

4.5.4. South American Countries 63
4.5.5. Asian Countries 64
Chapter 5: State-Sponsored Cyber Activities 65
5.1 Overview of The Main Global Cyber Conflicts 67
5.1.1 China vs Taiwan vs United States 67
5.1.2 Israel vs Iran 67
5.1.3 India vs Pakistan 68
5.1.4 Russia vs Ukraine 68
5.1.5 Other Theaters and Emerging Dynamics 69
5.2 Iran's Cyber Strategy: Doctrine, Capabilities, and Operations 69
5.2.1 Strategic Overview of Iran's Cyber Activities 69
5.2.3 Contracting Ecosystem 71
5.2.4 Operational Objectives and Tactics 72
5.2.5 Target Profile and Geographical Focus 72
5.2.6 Evolution and Trends in Iran's Cyber Capabilities 73
5.3 China's Cyber Strategy: Doctrine, Capabilities, and Operations 73
5.3.1 Strategic Overview of Iran's Cyber Activities 73
5.3.2 China's Cyber Power: Key Institutions and Structure 74
5.3.3 Contracting Ecosystem 77
5.3.4 Operational Objectives and Tactics 77
5.3.5 Target Profile and Geographical Focus 78
5.3.6 Evolution and Trends in China's Cyber Capabilities 78
5.4 Russia's Cyber Strategy: Doctrine, Capabilities, and Operations 78
5.4.1 Strategic Overview of Russia's Cyber Activities 78
5.4.2 Russia's Cyber Power: Key Institutions and Structures 79
5.4.3 Contracting Ecosystem 82
5.4.4 Operational Objectives and Tactics 82
5.4.5 Target Profile and Geographical Focus 82
5.3.6 Evolution and Trends in Russia's Cyber Capabilities 83
5.5 North Korea's Cyber Strategy: Doctrine, Capabilities, and Operations 83
5.5.1 Strategic Overview of North Korea's Cyber Activities 83
5.5.2 North Korea's Cyber Power: Key Institutions and Structures 83
5.5.3 Contracting Ecosystem 85
5.5.4 Operational Objectives and Tactics 85
5.5.5 Target Profile and Geographical Focus 86
5.5.6 Evolution and Trends in North Korea's Cyber Capabilities 86
5.6 Israel's Cyber Strategy: Doctrine, Capabilities, and Operations 87
5.6.1 Strategic Overview of Israel's Cyber Activities 87
5.6.2 Israel's Cyber Power: Key Institutions and Structures 87
5.6.3 Contracting Ecosystem 89

5.6.4 Operational Objectives and Tactics 90
5.6.5 Target Profile and Geographical Focus 90
5.6.6 Evolution and Trends in Israel's Cyber Capabilities 90
5.7 US Cyber Strategy: Doctrine, Capabilities, and Operations 91
5.7.1 Strategic Overview of the United States' Cyber Activities 91
5.7.2 United States' Cyber Power: Key Institutions and Structures 91
5.7.3 Contracting Ecosystem 92
5.7.4 Operational Objectives and Tactics 93
5.7.5 Target Profile and Geographical Focus 93
5.7.6 Evolution and Trends in the United States' Cyber Capabilities 93
Chapter 7: Disinformation and Information Warfare 94
7.1 The Strategic Evolution of Disinformation in the Cyber Domain 94
7.2 Geopolitical Motives and State Actors 95
7.3 Cyber Infrastructure and the Weaponization of Platforms 95
7.4 Tactics, Techniques, and Procedures (TTPs) 97
7.5 The Psychological and Societal Impact 98
7.6 Detection, Attribution, and Countermeasures 98
7.7 The Future Trajectory of Information Warfare 99
Chapter 8: Cyberterrorism and Hacktivism 99
8.1 Introduction to Cyberterrorism 99
8.2 Cyber Terrorism and Radical Islamist Organizations 101
8.3 Use of Cyberspace by Radical Islamist Organizations 102
8.3.1 Social Networks 102
8.3.2 Encrypted Messaging Applications 104
8.3.4 Darknet 108
8.4 Key Terrorist Organizations and Their Cyber Activities 109
8.4.1 Hamas 109
8.4.2 Hezbollah 116
8.4.3 Islamic State (ISIS/ISIL) 121
8.4.4 Al-Qaeda 127
8.5 Hacktivism 132
8.5.1 Prominent Hacktivist Groups 133
8.5.2 Cooperation Between Hacktivists and Cybercriminals 136
Part III: Cyber Geopolitics and Alliances 140
Chapter 9: Cyber Diplomacy in a Multipolar World 140
Chapter 10: International Cybersecurity Framework and Alliances 141
Chapter 11: The Global Cyber Arms Race and Power Projection 142
11.1 AI, Quantum Computing, and Next-Generation Warfare 142
11.2 Cyber Arms Market 143
11.3 Ethics, Escalation Risks, and Global Cyber Stability 145
Part IV: Innovations and Cyber Strategy 146

Chapter 12: The Private Sector as a Cyber Power **146**
Chapter 13: Cyber Strategy in the Age of AI and Quantum Computing **147**
Chapter 14: Innovation Models from Global Cyber Hubs **148**
14.1 Estonia: The Digital State Built on Resilience **148**
14.2 Israel: Where National Security Meets Cyber Startups **148**
14.3 Singapore: Securing the Smart Nation **149**
14.4 South Korea: Industrial Protection and Public-Private Unity **149**
14.5 The Netherlands: The Global Connector **149**
Chapter 15: Strategic Frameworks and Doctrines in Cybersecurity **150**
15.1 National Cyber Strategies: A Mirror of Geopolitical Identity **150**
15.2 Military vs. Civilian Cyber Doctrines: Dual Lenses of Power **151**
Chapter 16: Cyber Resilience and Strategic Infrastructure Protection **154**
Chapter 17: Future Scenarios and Strategic Foresight in Cyberspace **158**
Conclusion **160**
Bibliography **161**
About the Author **165**

Introduction

The 21st century has brought a revolution unlike any before one, driven not by steam or steel, but by networks, algorithms, and data. A new strategic domain has emerged: cyberspace. Once a niche experiment born from Cold War collaboration between universities and the military, cyberspace has grown into a vast, interconnected digital ecosystem. Today, it is as vital and contested as land, sea, air, and space. Every aspect of modern life, commerce, communication, governance, warfare, and even ideology, is now intertwined with the digital realm. But with this deep integration comes growing vulnerability. As our lives increasingly move online, the threats follow. Cyberspace is built on physical and logical infrastructure: undersea cables, satellites, routers, and protocols. Yet it is shaped just as much by human behavior. How people, institutions, and societies act online determines how power and risk evolve in this new domain.

Cyberspace has become a battleground populated by various actors, including corporate, criminal, and state. Among the most active are cybercriminals: organized, agile, and global. Operating through encrypted channels and dark web marketplaces, they exploit digital weaknesses using phishing, ransomware, spyware, and data breaches. Their operations are constantly evolving, and their impact is widespread. However, cybercrime is only one dimension. Nation-states increasingly engage in digital warfare, using cyberspace to sabotage infrastructure, steal intelligence, manipulate public opinion, and weaken adversaries without firing a single shot. Leading cyber powers, including the United States, China, Russia, Iran, North Korea, and Israel, are shaping a new era of global conflict through covert and often deniable operations. Alongside cyberattacks, a parallel form of warfare has emerged: the weaponization of information. Disinformation campaigns, influence operations, and psychological tactics distort truth, sow division, and undermine trust in democratic systems. Social media platforms, once seen as tools for empowerment, are now strategic battlegrounds for manipulation.

Non-state actors also play a significant role. Extremist groups, terrorist organizations, and hacktivists use the digital space to recruit, spread propaganda, and launch disruptive attacks. The line between activism and terrorism, dissent and sabotage, is becoming harder to define. In this volatile landscape, the global balance of power is shifting. While international efforts are underway to govern cyberspace, existing frameworks remain incomplete and fragile. A new arms race is unfolding, measured not in missiles but in software exploits, artificial intelligence, and digital influence.
Emerging technologies like AI, quantum computing, and next-generation networks are transforming cyberspace's possibilities and risks. Private companies now wield much technological power and control critical infrastructure, making them central players in this evolving domain. The challenge ahead is clear: how can we build resilience in the face of persistent cyber threats? What strategies, alliances, and safeguards are needed to secure this domain? And what kind of future are we

creating intentionally or not through our growing dependence on digital systems? Understanding cyberspace is essential for anyone seeking to grasp the shifting architecture of global power. It is not just a technical or military issue, but a political, economic, psychological, and existential one. To understand cyberspace is to understand the century we now live in.

Part I: Understanding the Cyber Sphere

Chapter 1: Origins of Cyberspace

1.1 From ARPANET to Global Internet

The foundation of today's digital world was laid decades ago amid the geopolitical tensions of the Cold War, driven by a critical need for secure and resilient communication. In the late 1960s, the U.S. The Department of Defense's Advanced Research Projects Agency (DARPA) initiated ARPANET, a groundbreaking collaboration between the military and academia. Its goal was to create a communication network to withstand a nuclear strike. At the heart of this effort was the innovative concept of packet switching, which allowed data to be divided into packets and transmitted across multiple routes, ensuring the network's survival even if parts were destroyed. Starting with just four connected sites in 1969, ARPANET laid the foundation for decentralized digital communication. By the early 1980s, the introduction of the TCP/IP protocol enabled different networks to connect and communicate, transforming ARPANET into the scalable, interconnected system that would become the Internet.

The 1990s introduced the World Wide Web, invented by Tim Berners-Lee, which layered hypertext navigation on top of the internet infrastructure, turning technical connectivity into a usable, visual experience for the average person. Commercial browsers like Netscape democratized access, enabling individuals and businesses to create and explore websites. The general public was observing and participating in the digital sphere for the first time. Email replaced traditional correspondence, search engines curated the world's information, and a once-military experiment became the backbone of a new global economy. As this connectivity deepened, cyberspace emerged as a communications platform and a parallel domain of existence, where people worked, learned, played, and began to live portions of their social and emotional lives.

The early 2000s ushered in the era of Web 2.0, where the internet evolved from a static library to an interactive platform. Social networking sites like Friendster, MySpace, and Facebook catalyzed this transformation. No longer was the internet a passive experience; users became content creators, forming digital identities, communities, and economies. These platforms shifted the paradigm from anonymity to hyper-personalization. People began sharing their thoughts, activities, photos, and locations in real time. This self-disclosure transformed human interaction and provided the foundation for surveillance capitalism, where personal data became a commodity. With the proliferation of mobile devices and constant connectivity, cyberspace ceased being a "place one visits" and became a pervasive layer of life, increasingly indistinguishable from the physical world.

1.2 Evolution into a Strategic Domain

Cyberspace's journey from a cooperative academic project to a militarized and contested domain represents one of the most consequential transformations in modern geopolitical history. While the internet was initially designed with openness and redundancy in mind, this very openness has made it an attractive terrain for conflict. In the late 1990s and early 2000s, governments began to recognize the strategic importance of cyberspace as an enabler of command, control, and communication systems and as a battleground in its own right. The 2007 cyberattacks on Estonia, widely seen as the first instance of a coordinated digital assault on a nation-state, demonstrated that a country's economy, infrastructure, and information space could be paralyzed without firing a single bullet[11]. Since then, cyber operations have become routine tools of statecraft, espionage, and coercion[12].

Today, cyberspace is widely acknowledged as the fifth operational domain of warfare, alongside land, sea, air, and space. Major powers like the United States, China, Russia, and others have established dedicated cyber commands and embedded cyber doctrines into their military strategies. Offensive cyber capabilities have evolved to include not only data theft and surveillance but also sabotage of critical infrastructure, manipulation of public opinion through disinformation, and psychological operations at a mass scale. Non-state actors, ranging from hacktivist groups to criminal cartels and terrorist organizations, have also weaponized digital tools for ideological, financial, or disruptive ends[15]. In this way, cyberspace has become a gray zone of conflict, where attribution is difficult, norms are unclear, and actions often fall below the threshold of armed conflict yet carry significant consequences.

Simultaneously, cyberspace's strategic value has extended into the economic and ideological realms. Control over digital infrastructure, platforms, and standards has become a form of soft power. Tech giants influence democratic processes, public discourse, and access to knowledge more than many governments do. Data, the raw material of the digital age has become more valuable than oil, prompting fierce competition over who collects, controls, and interprets it[17]. Artificial intelligence, quantum computing, and 5G technologies are now frontiers of geopolitical rivalry, as control over these systems equates to control over future capabilities in security, commerce, and societal influence[18].

1.3 The Rise of Digital Dependence

As cyberspace has expanded, it has become inextricably woven into the fabric of modern life, creating a profound and growing dependence on digital systems that shape how societies function and individuals navigate reality[19]. Access was limited in the early internet era, occasional, and often supplemental. Today, it is constant, expected, and foundational. Nearly every essential service, including banking, healthcare, education, transportation, and governance, now relies on uninterrupted digital connectivity. The smartphone revolution, catalyzed by Apple's iPhone in 2007 and affordable mobile internet access, put a supercomputer in billions of hands, enabling people to remain perpetually connected[21]. This 24/7 immersion has created a paradigm in which digital tools are no longer conveniences but extensions of cognition, memory, and identity.

The Internet of Things (IoT) has taken this dependency further by embedding sensors and processors into physical objects, from refrigerators and thermostats to cars and city infrastructure, linking the digital and physical worlds into a single, responsive environment[23]. Smart homes, wearable health trackers, GPS navigation, and voice-activated assistants have redefined convenience while raising urgent questions about privacy, autonomy, and surveillance. Meanwhile, the rise of cloud computing has centralized data storage and processing power, allowing individuals and organizations to access vast capabilities with minimal local infrastructure[24]. But this centralization also introduces points of failure, massive data breaches, system outages, and vulnerabilities that can paralyze entire economies.

More recently, integrating blockchain technology and artificial intelligence has added new layers to this dependence. Decentralized systems like cryptocurrencies and smart contracts promise liberation from traditional financial institutions and intermediaries, yet they also create regulatory gray zones exploited by criminals and bad actors. AI now mediates everything from social media feeds and search results to hiring decisions and predictive policing, embedding algorithmic logic into human institutions. These developments offer efficiency and empowerment, but also introduce opaque, systemic risks. Disinformation campaigns, deepfakes, and social engineering have demonstrated how easily digital ecosystems can be manipulated, undermining trust in truth[28]. Ultimately, the rise of digital dependence represents more than a technical shift; it is a civilizational transformation. Cyberspace is no longer external to human life; it is a constitutive part of it. Our identities are shaped through digital footprints, decisions guided by algorithmic nudges, and relationships often initiated and maintained through screens[29].

Chapter 2: Anatomy of the Digital World

The Internet is a vast, interconnected network with various essential components that interact to enable communication and data exchange. At the heart of this structure are hosting servers, which store websites, applications, and data, making them accessible to online users[30]. These servers respond to client requests and deliver the requested content. Routers are vital in routing data packets between different networks, ensuring they reach their destination most efficiently[31]. DNS (Domain Name System) servers function like the Internet's phone book, translating user-friendly domain names (such as www.example.com) into IP addresses that allow machines to identify themselves[32].

Additionally, clients, such as personal computers or smartphones, initiate requests for information or services, while ISPs (Internet Service Providers) provide the infrastructure and access necessary to connect to the Internet[33]. The Internet infrastructure comprises a complex hardware, software, protocols, and services set[34]. Here's a breakdown of the key elements:

2.1 Physical Infrastructure

These are the foundational elements that physically support the Internet:

- **Data Centers:** Facilities housing servers that store and process web content (both surface and deep web).
- **Servers:** Machines hosting websites, databases, and services (e.g., web servers, mail servers, FTP servers).
- **Routers & Switches:** Devices that manage and direct data traffic between networks.
- **Cabling (Fiber Optics, Ethernet):** High-speed cables that transmit data globally.
- **Internet Exchange Points (IXPs):** Hubs where different networks interconnect to exchange traffic.

2.2 Network Infrastructure

Protocols and services that manage data transfer:

- **IP Addresses & DNS:**
    - **IP (Internet Protocol):** Identifies devices on the network.
    - **DNS (Domain Name System):** Translates human-readable domain names to IP addresses.
- **BGP (Border Gateway Protocol):** Manages how packets are routed across the Internet through ISPs.

- **TCP/IP:** Core suite of communication protocols used to interconnect devices on the Internet.

2.3 Access Infrastructure

These components enable end-users to connect to the Internet:

- **Internet Service Providers (ISPs):** Companies that provide Internet access to homes and businesses.
- **Modems & Routers:** Devices at the user premises enabling connection to the ISP.
- **Mobile Networks & Wi-Fi:** Wireless means to access the Internet.

2.4 Web Infrastructure

This supports access to the surface web (indexable by search engines) and deep web (not indexed):

- **Web Servers (e.g., Apache, Nginx):** Serve HTTP/S content.
- **Databases (e.g., MySQL, MongoDB):** Store and manage data that supports dynamic content (much of which forms the deep web).
- **Content Management Systems (CMS):** Platforms like WordPress and Drupal are used to manage websites.
- **Search Engines (e.g., Google, Bing):** Index and retrieve surface web content.

2.5 Application & Protocol Layer

Used to access both the surface and deep web:

- **HTTP/HTTPS:** Protocols used to access web pages.
  FTP/SFTP: Used for file transfer.
- **APIs (REST, GraphQL):** Interface to access data programmatically (often deep web).
- **Authentication Systems:** Control access to restricted content (deep web), like login portals.

2.6 Security Infrastructure

Vital for secure access and data protection:

- **SSL/TLS Certificates:** Enable secure (HTTPS) connections.
- **Firewalls & Intrusion Detection Systems:** Protect servers and networks.
- **VPNs & Proxies:** Used for private, secure access (sometimes to deep or restricted content).

Within cyberspace, we distinguish three layers, including the surface web, the deep web, and the dark web (Figure 1).

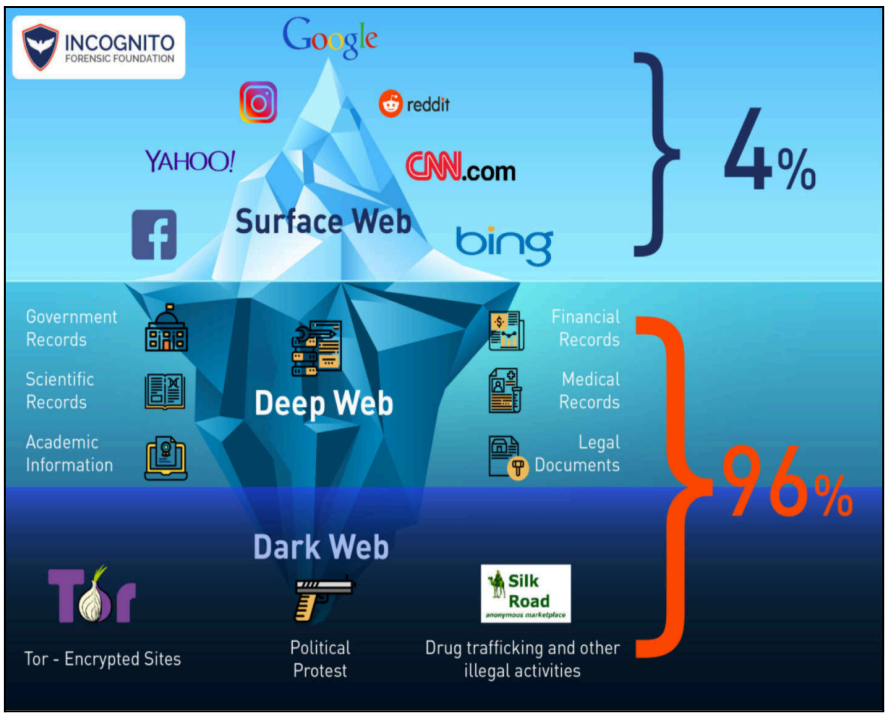


Figure 1 - Cyberspace layers

The surface web encompasses the portion of the internet easily accessible to the public via standard web browsers and popular search engines such as Google Chrome, Internet Explorer, or Firefox. This layer provides access to widely used open platforms and resources like Facebook, YouTube, Instagram, and Gmail. Various malicious actors operate on the surface web, exploiting its accessibility to achieve multiple goals.

The deep web refers to the most significant portion of the internet not indexed by traditional search engines such as Google. Approximately 90% of internet sources must be indexed by Google. Many web pages are considered part of the deep web because they do not use common top-level domains (TLDs), such as .com, .co, and .org, and are not indexed by traditional search engines. Deep web sources like online banking, email servers, or private social media pages typically require restricted access. From an infrastructure perspective, Deep Web websites are accessible via traditional URLs or IP addresses; however, they may need access to public web pages via secure access.

The Dark Web refers to hidden networks that exist beneath the surface of the traditional internet and are accessible only through specialized software. The Onion Router (Tor) and the Invisible Internet Project (I2P) are among the most widely used platforms enabling access to these networks.

These tools allow users to visit unindexed websites, often cataloged by specific repositories or specialized search engines, with the primary goal of ensuring anonymity and data confidentiality through sophisticated encryption techniques. Tor and I2P are gateways to different anonymized networks within this hidden web layer, with Tor being the most prominent and widely used. The Tor network operates on a decentralized, volunteer-based model. Users who wish to contribute actively rather than simply browse can run a script on their machines to transform them into nodes within the network. These nodes form the infrastructure that relays encrypted traffic across the network. Notably, each node in Tor knows only the immediate destination of the data, not its whole route, which enhances privacy (Figure 2). Tor's architecture consists of three types of nodes: entry, middle, and exit. Like routers on the traditional internet, these nodes pass data along a dynamically generated path that changes with each new request, reinforcing the user's anonymity (Figure 3).

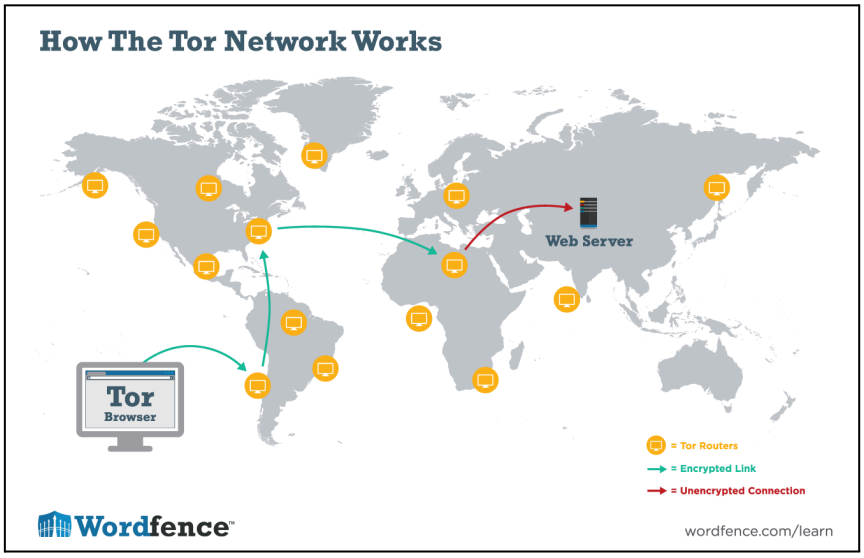


Figure 2 - ToR Network World Map

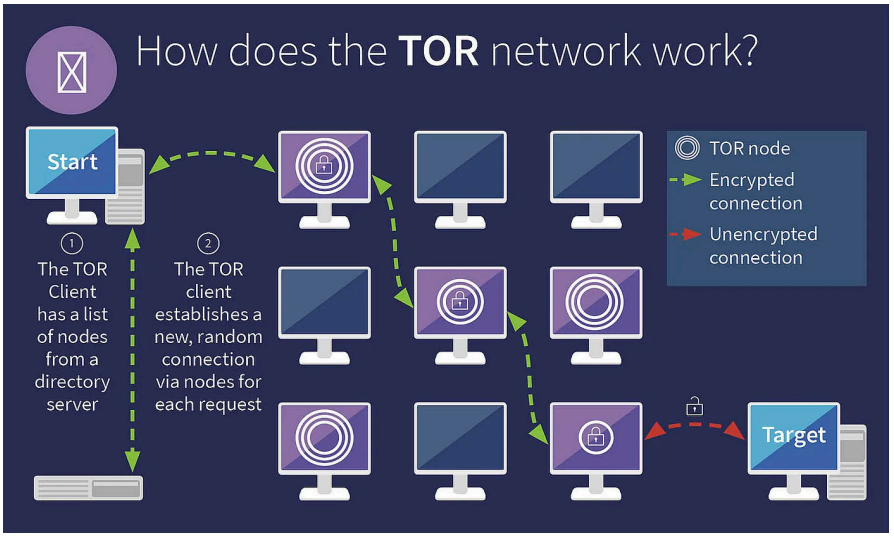


Figure 3 - TOR network structure

The I2P network is composed of nodes known as "routers," which are linked through one-way virtual paths called "tunnels" (as illustrated on the tunnel routing page). Each router has a unique and typically persistent cryptographic identity known as a RouterIdentity. Routers communicate by using standard transport protocols such as TCP and UDP. Client applications are assigned their cryptographic identifiers, called destinations, enabling them to send and receive messages. These clients can connect to any router and request a temporary allocation of tunnels referred to as leases, which transmit messages securely across the network (Figure 4).

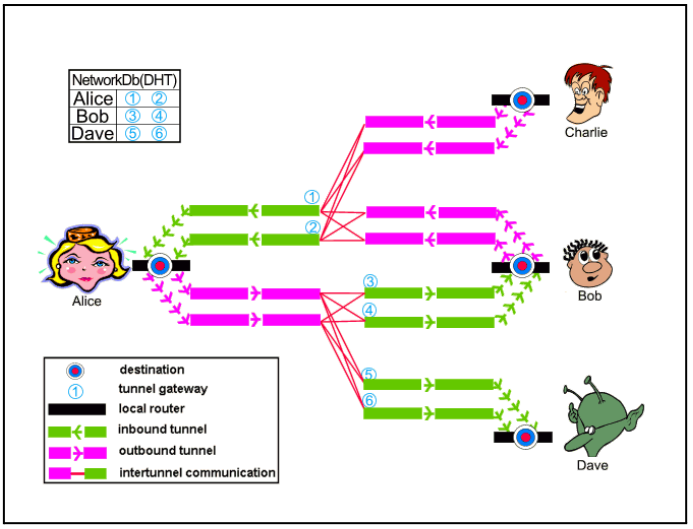


Figure 4 - I2P network structure

Beyond the foundational components of cyberspace, such as servers, routers, switches, and transmission media, the modern digital ecosystem has evolved into a vast, multifaceted domain incorporating a wide range of advanced technologies and systems. One significant development is the proliferation of Internet of Things (IoT) devices, which include everyday objects such as smart thermostats, surveillance cameras, industrial sensors, and even medical implants, all of which contribute real-time data and computational power to the broader network[35]. Additionally, the emergence of cloud computing infrastructure, such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform, has dramatically shifted the architecture of cyberspace from localized, static data centers to globally distributed, scalable platforms that support data storage, processing, and software deployment across virtualized environments[36]. Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, often overlooked in general cyber discussions, are vital components of cyberspace, particularly in energy, water, manufacturing, and transportation sectors. These systems connect the digital world with physical operations, introducing both efficiency and unique vulnerabilities[38]. On a larger scale, national and governmental infrastructures have played a crucial role in shaping cyberspace.

This includes sovereign internet architectures, like China's Great Firewall, Russia's Runet, and secure communication backbones such as the U.S. Department of Defense's Global Information Grid (GIG) or Europe's GAIA-X project[39]. These infrastructures are designed for data transmission, control, surveillance, and cyber defense, emphasizing digital sovereignty and security[40]. Furthermore, the rise of content delivery networks (CDNs), satellite internet constellations like Starlink, and undersea fiber optic cables as geopolitical assets all contribute to a complex, layered, and dynamic cyberspace deeply entwined with civil and strategic national interests.

Chapter 3: Behavior in the Digital Age

3.1 Human Online Behaviour

The rapid growth and global reach of cyberspace have given rise to a new digital lifestyle. As goods and services are increasingly digitized, human behavior evolves, demanding constant adaptation. In January 2025, Kepios published its annual report, offering valuable insights into how the global population engages with the internet, primarily through smartphones and social media platforms (Figures 5 and 6). The findings reveal that a majority of the world's population is now connected to digital life, either directly or indirectly. The study also outlines the primary purposes for internet use and includes statistics on how frequently people open social media apps daily (Figures 7 and 8).

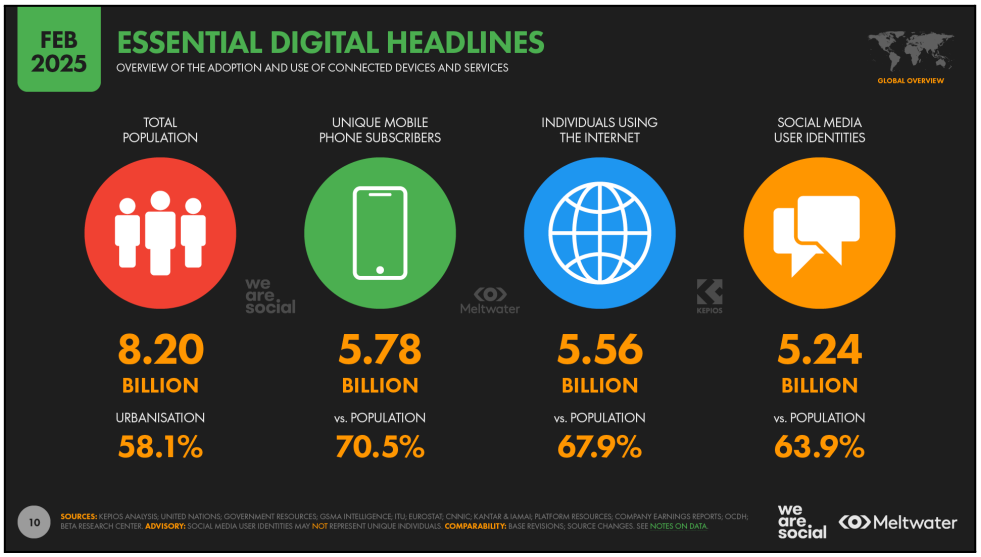


Figure 7 - Global essential digital headlines in 2025 (Source: –Kepios)

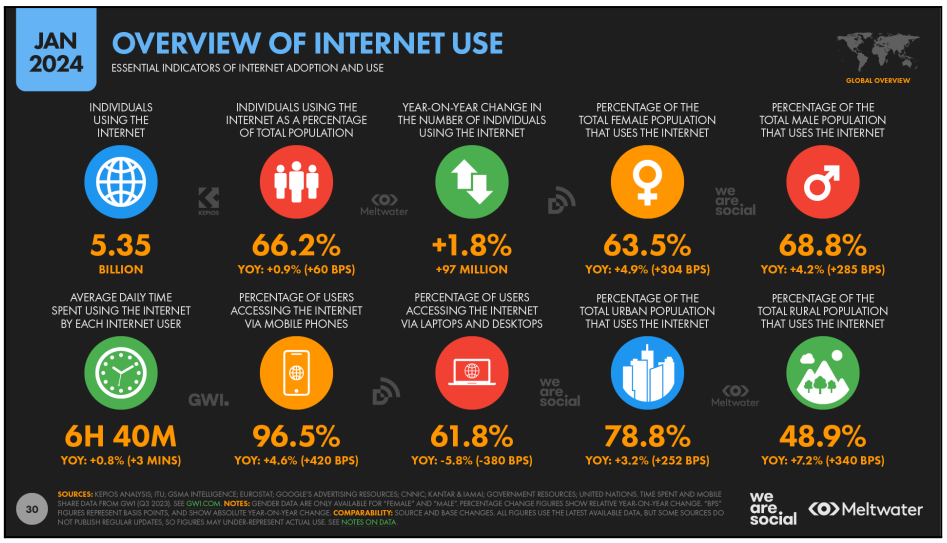


Figure 6 - Global overview of Internet use in 2024 (Source: Kepios)

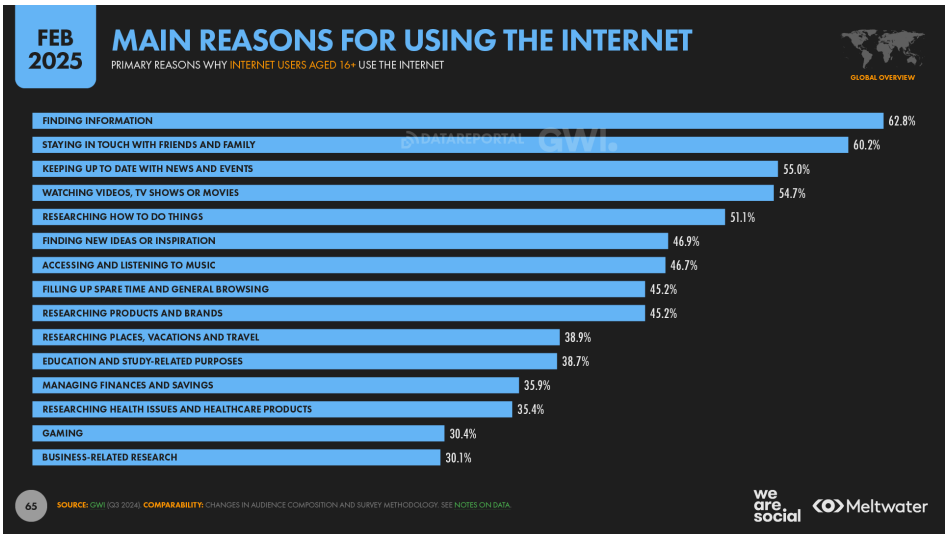


Figure 7 - Global main reasons for using the Internet in 2025 (Source: Kepios)

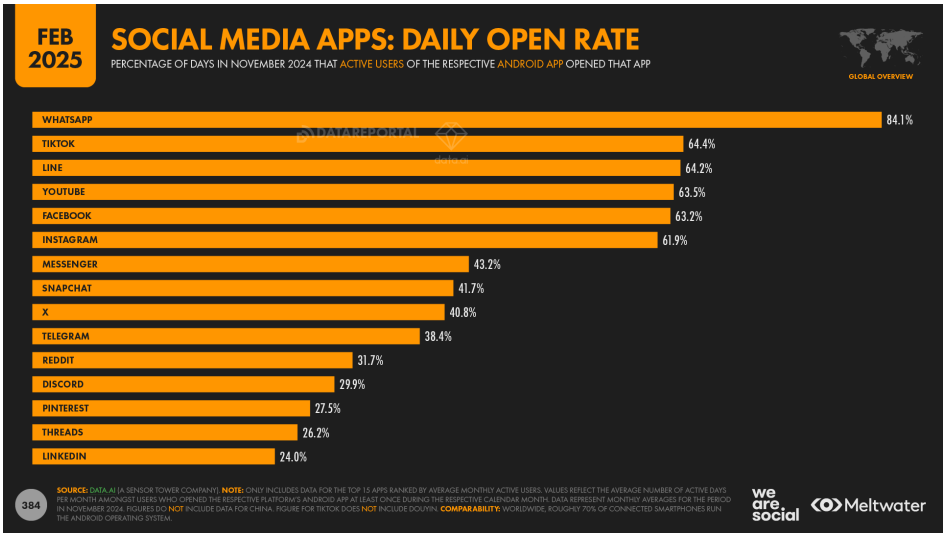


Figure 8 - Global social media application daily open rate in 2025 (Source: Kepios)

Human-machine interaction (computers, smartphones, tablets, cameras, ATMs, cash registers, etc.) is now ubiquitous, resulting in very different human-to-human interactions. The development of social media and applications has fundamentally changed human behavior. Indeed, this expansion of cyberspace and the sharp increase in accessible information and data significantly impact humans. It's often difficult for humans to assimilate a large amount of data daily and extract and understand the essentials without getting lost in the mass.
The spread of fake sites, fake news, and fake data only complicates this interaction between humans and machines.

In 2018, a landmark study by three researchers at the Massachusetts Institute of Technology revealed a troubling dynamic in the digital information ecosystem: false news spreads significantly faster on the social platform X (formerly Twitter) than factual reporting and by a considerable margin.[42] This revelation sparked a wave of subsequent research from institutions worldwide, including a notable study from the University of Southern California.[43] These investigations have increasingly pointed to the structural design of social media platforms as a key driver of misinformation. By rewarding the act of sharing, these platforms inadvertently prioritize virality over veracity. According to the USC researchers, misinformation gains traction because users may lack the critical thinking skills necessary to discern truth from falsehood, and because entrenched ideological convictions often cloud objective judgment.

At the same time, the growing presence of artificial intelligence in everyday life introduces a dual-edged phenomenon. While AI brings about remarkable advancements and efficiencies, it also presents significant risks particularly in its potential for misuse. With alarming ease, AI can now be deployed to generate and disseminate large volumes of fabricated or misleading content, bypassing traditional mechanisms of verification and accountability.[44] The consequences extend beyond the spread of false information: AI-powered tools now enable the realistic simulation of a person’s voice or image, making identity theft and deception more sophisticated.

A broader behavioral trend compounds these developments: our collective desire to navigate the digital world rapidly. The relentless consumption of online content, whether through websites, social media platforms, apps, or streaming services, has dulled our vigilance. Even in critical contexts, such as accessing banking or government services, users may fail to pause and scrutinize what they are engaging with. Users remain vulnerable despite the widespread adoption of safeguards such as multi-factor authentication. Their susceptibility often stems not from a lack of security tools, but from a deeper human impulse: the tendency to prioritize convenience over caution.

3.2 Impact on Cyber conflicts

As human behaviour increasingly migrates into the digital realm, it reshapes how we interact and communicate and how we engage in conflict. The evolution of cyber conflict is deeply intertwined with this behavioural shift. In the early days of the internet, cyber incidents were primarily driven by curiosity, mischief, or personal agendas, manifesting as isolated acts of hacking and digital vandalism by individuals or small groups. However, as society became more dependent on digital systems for governance, commerce, and social interaction, the stakes of online behaviour escalated. The growing digital footprint of individuals and institutions created new vulnerabilities and opportunities, prompting nation-states to notice. What began as scattered online disruptions evolved into sophisticated, state-backed operations leveraging the same platforms where people connect, share, and live increasingly virtual lives.

The 2007 cyberattacks on Estonia, sparked partly by socio-political tensions and amplified by the online behaviours of various actors, marked a turning point: a national crisis unfolding entirely in cyberspace. The emergence of tools like Stuxnet, capable of causing real-world damage through digital means, underscored the strategic potential of cyber operations. Since then, the line between civilian digital activity and military-grade cyber operations has blurred. Human actions, whether through the spread of disinformation, participation in hacktivist movements, or even careless digital habits, have become both targets and vectors in cyber conflict. As technologies such as artificial intelligence and machine learning further integrate into daily life, they also expand the landscape of cyber threats, turning everyday behaviour into potential leverage points for state and non-state actors. Thus, the trajectory of cyber conflict is not solely a story of advancing technology, but a reflection of how human behaviour in cyberspace has redefined the nature of aggression, defense, and power in the modern world.

Part II: Cyber Warfare: Crime, Conflict, and Control in a Digital World

Chapter 4: Cybercrime Ecosystem and Operations

The cybercrime ecosystem has rapidly transformed from a fragmented landscape of lone hackers into a sophisticated, interconnected, and resilient global economy of digital crime. This shadowy network now mirrors many aspects of the legitimate business world, complete with supply chains, service providers, customer support, and performance guarantees. Cybercriminals operate within a decentralized structure, where roles are specialized and tasks are outsourced, ranging from malware creation and exploit development to laundering stolen assets and trafficking in illicit data. Cybercriminals rely on underground forums, darknet marketplaces, and encrypted communication platforms to collaborate, trade tools and information, and conceal their identities from law enforcement. Cybercrime-as-a-service (CaaS) models have increasingly lowered the technical barrier to entry, enabling less skilled individuals to orchestrate complex attacks through rented botnets, ransomware kits, and phishing campaigns. Moreover, geopolitical tensions and economic instability have fueled a surge in state-sponsored and ideologically motivated cyberattacks, further blurring the lines between cybercrime, cyber warfare, and cyberterrorism. This chapter introduces the architecture and inner workings of the cybercrime ecosystem, offering a high-level overview of its actors, motivations, and operational frameworks. It lays the groundwork for a detailed analysis of the tools, tactics, and infrastructures that sustain its growth and resilience in the face of evolving cybersecurity efforts.

4.1 Cybercriminal Platforms

The cybercrime ecosystem is vast and varied. Cybercriminals usually operate in multiple playgrounds depending on their activities and modus operandi. Several criminal platforms exist, including forums, auto-selling marketplaces, black markets, and crypto messaging apps. These online crime platforms are generally easily accessible. However, some require privileged access, which can be obtained by payment or contact.

4.1.1 Forums

Cybercriminal forums are among the most significant platforms facilitating illicit activities online. Numbering in the hundreds, these forums vary widely regarding user engagement and the types of criminal enterprises they support. Found across both the surface web and the dark web, they exist in multiple languages and cater to nearly every form of cybercrime imaginable (Figure 8). Within this sprawling digital underworld, forums can be broadly grouped into three main categories. The first includes technical forums, where threat actors trade malware, exploits, and other offensive tools (Figure 9). The second category revolves around access and data markets, where users buy and sell compromised network access and stolen databases (Figure 10). Finally, financial fraud and carding forums focus on payment fraud schemes, including stolen credit card data and identity theft (Figure 11).

These platforms often feature organized sections such as malware, databases, fraud, and marketplaces, each serving specific functions within the forum. Access levels vary depending on the forum's internal policies. Some allow public browsing, while others require registration, typically involving only a pseudonym and email address. More exclusive forums, especially those dealing with high-value or sensitive material, often restrict access behind paywalls or through invite-only systems, sometimes requiring vouches from existing members. These gatekeeping mechanisms serve not only to manage community size but also to deter casual users and script kiddies, thereby fostering a space more conducive to serious cybercriminal collaboration.



Figure 8 - Link Base worldwide cybercriminal forums repository

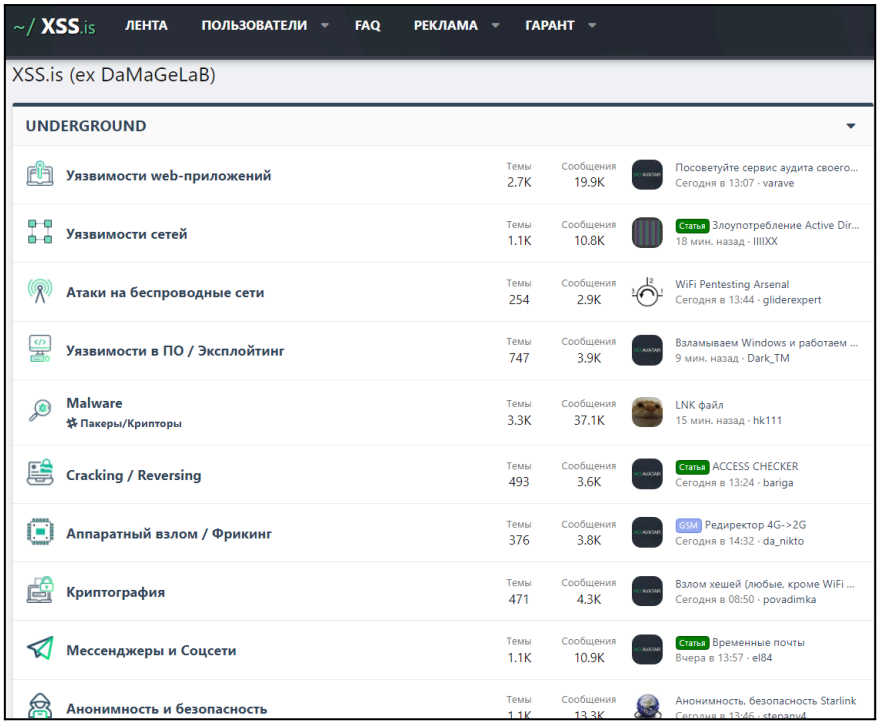


Figure 9 - One of the most popular Russian-speaking technical hacking forums (XSS.IS)

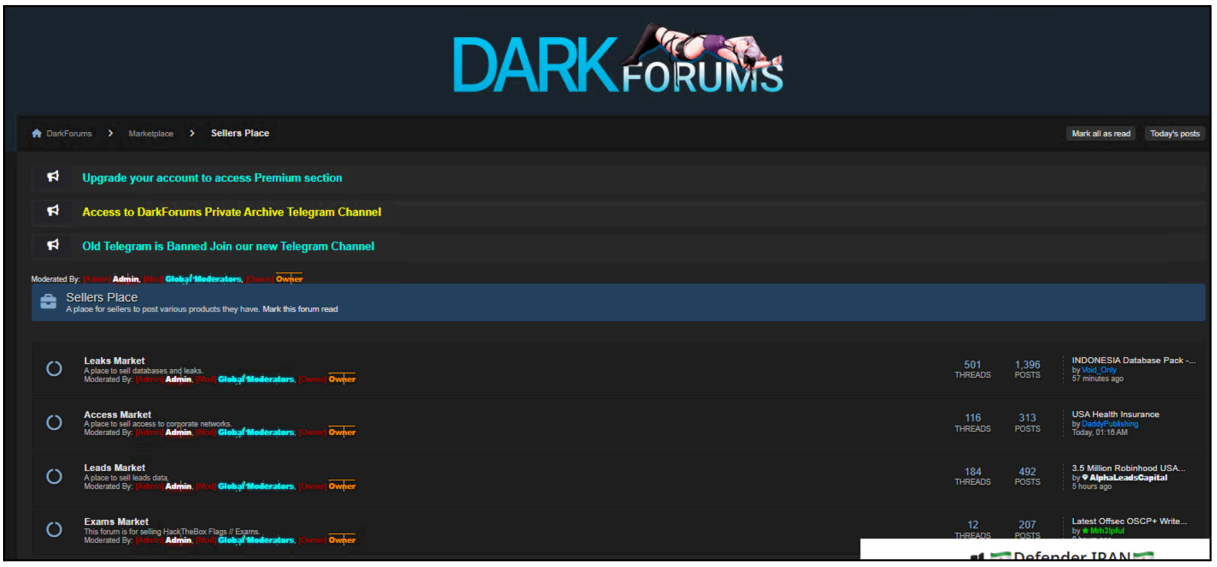


Figure 10 - A popular data leak forums (Darkforums)

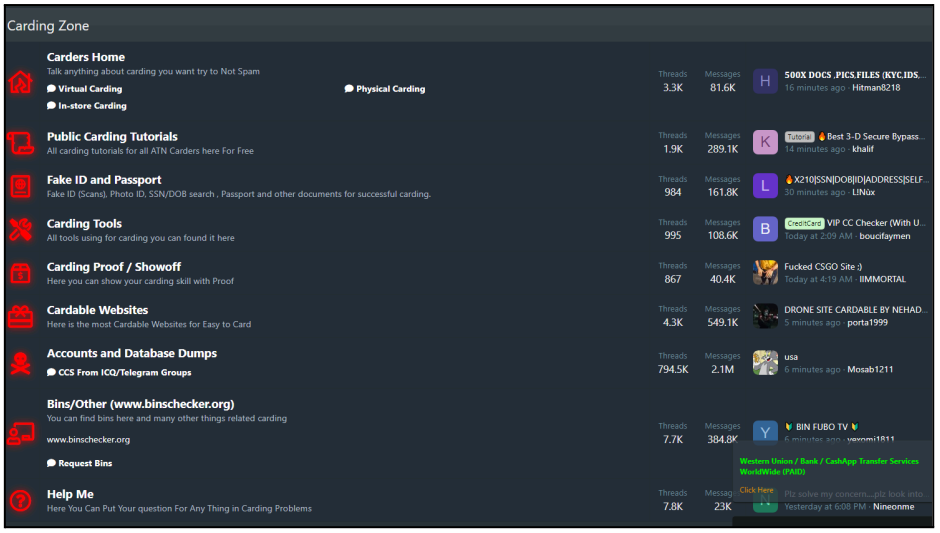


Figure 11 - A well-known English-speaking carding forum (Altenen Carding)

The management of cybercrime forums is generally based on a hierarchical structure with actors among the following:

- **Administrator** (aka admin): He manages the operations and administers the forum (Figure 12).
- **Moderator** (aka mod): There are usually several, depending on the forum size. They generally manage one of the multiple criminal sections of the forum (malware, databases, fraud...) (Figure 13).
- **VIP user:** This type of user usually has access to more sections on the forum (with more exclusive content) by paying fees (Figure 14).
- **User**: Refer to the majority of people registering on the forum.

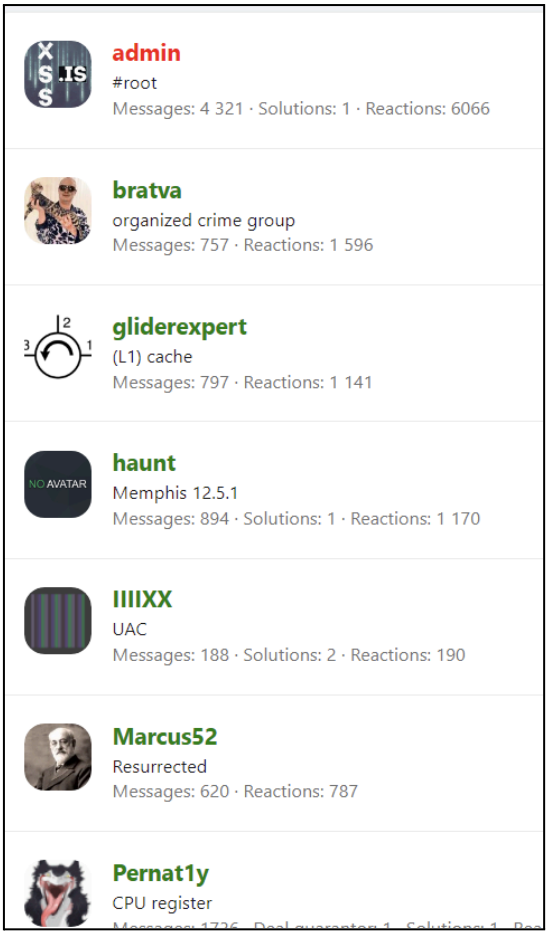


Figure 12 - List of Admin and moderators on a Russian hacking forum (xss.is)



Figure 13 - Moderator recruitment post on a carding forum (Altenen forum)



Figure 14 - Upgrade user packages for sale on a hacking forum (Leakzone forum)

4.1.2 Automatic Selling Marketplace

The Automatic Selling Marketplace represents a sophisticated online infrastructure to facilitate the automated exchange of stolen digital assets. Typically run by organized cybercriminal groups, these platforms leverage expansive botnet networks of tens of thousands of compromised devices to harvest and distribute illicit data. Designed for minimal oversight, these marketplaces allow users to browse and purchase stolen assets without direct interaction with administrators. Despite minor variations, most of these platforms share a typical architecture. At their core is a robust database housing large volumes of stolen data, including credit card information, bank account credentials, and application logins. A user-friendly control panel enables buyers to filter results by criteria such as card type, issuing bank, or country of origin. Transactions are conducted using cryptocurrency, requiring users to maintain a positive account balance. Once an asset is selected, the platform executes the transaction automatically, deducting the appropriate amount from the user's balance. (Figures 15, 16, and 17).

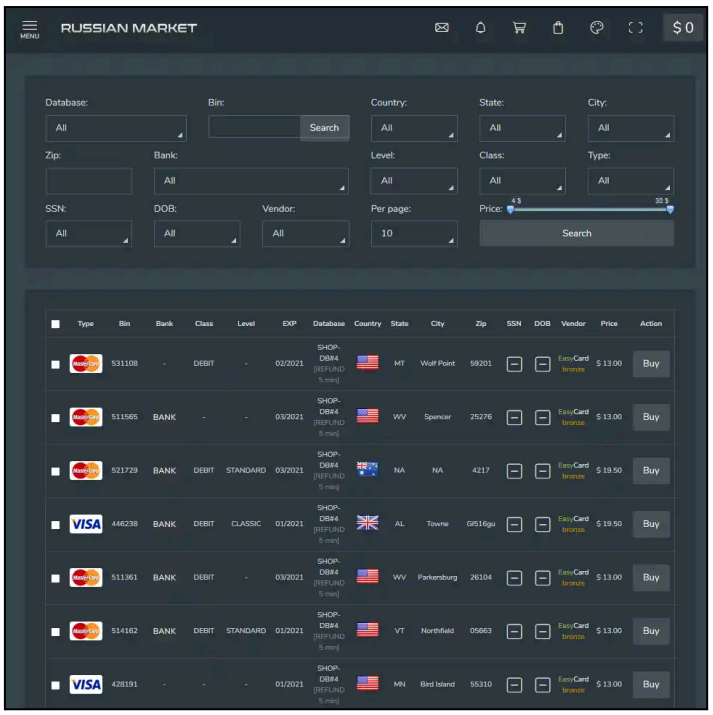


Figure 15 - Automatic Selling Credit Cards Russian Market

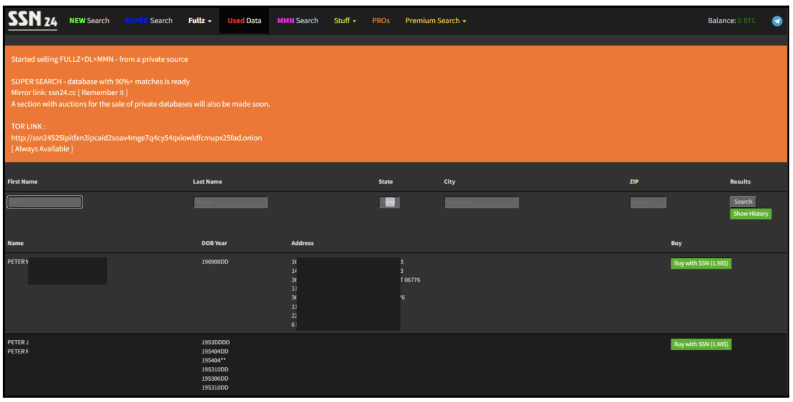


Figure 16 - Automatic selling PII market

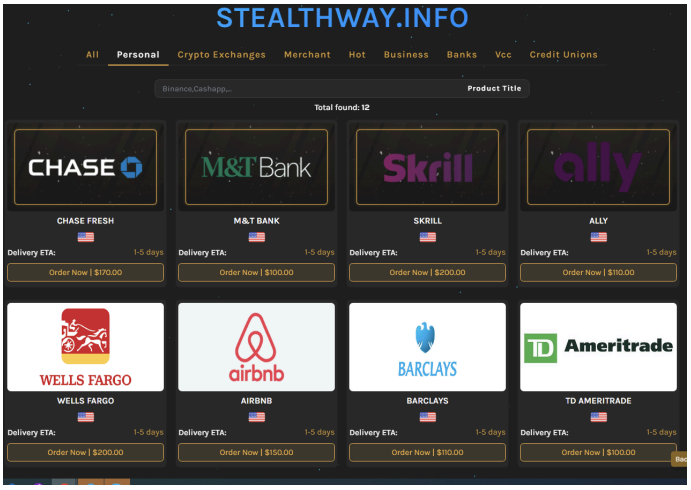


Figure 17 - Automatic selling market Bank accounts

4.1.3 Underground Markets

Underground markets provide cybercriminals a platform to trade a wide range of illicit goods and services. Depending on the market's infrastructure, vendors may operate individual storefronts or conduct sales through centralized systems. Commonly offered items include narcotics, firearms, counterfeit documents and currency, stolen credit card information, banking credentials, exploit kits, malware, personal identity data, and unregulated pharmaceuticals. Vendors typically maintain detailed profiles showcasing their product listings and often include a PGP (Pretty Good Privacy) key to facilitate secure communication with buyers. Transactions are generally conducted using cryptocurrency, which is transferred to designated wallets within the marketplace. Most markets feature rating systems, allowing buyers to evaluate vendors based on product quality and service reliability. However, these systems can be manipulated; some sellers create multiple accounts and post fraudulent reviews to boost their reputation artificially. It's also important to note that scams are widespread, and not all advertised products exist (Figures 18, 19, and 20).

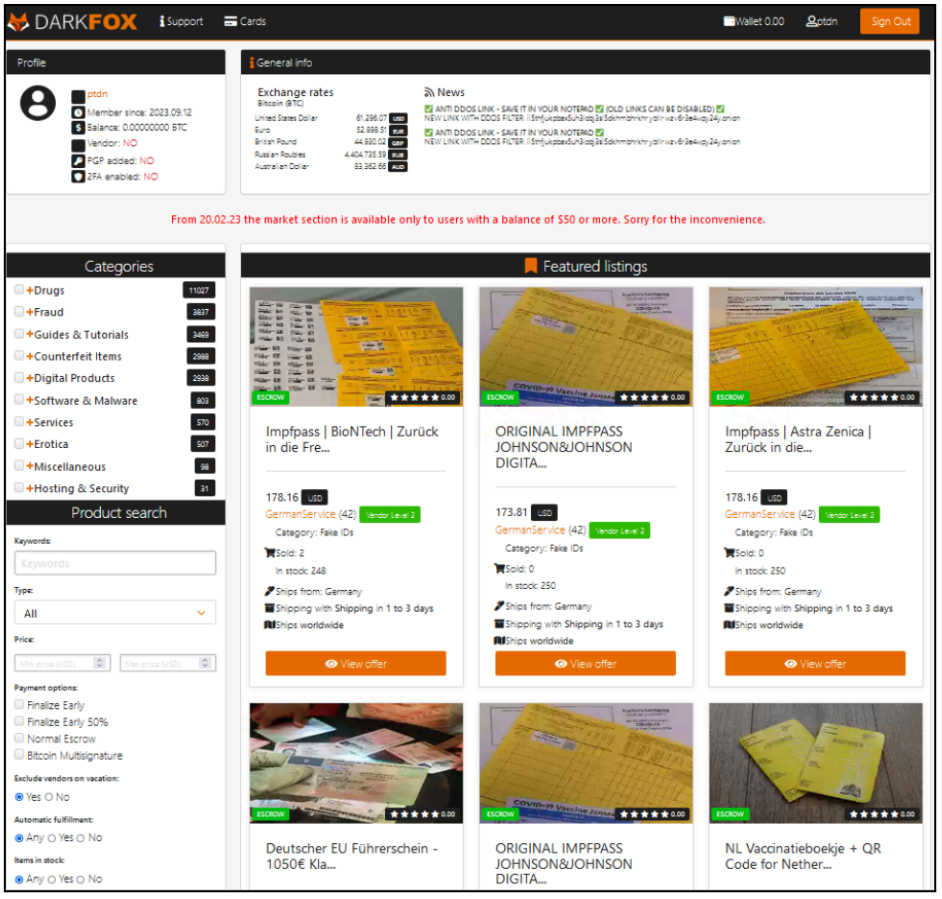


Figure 18 - Example of a darknet criminal market (Source: Darkfox)

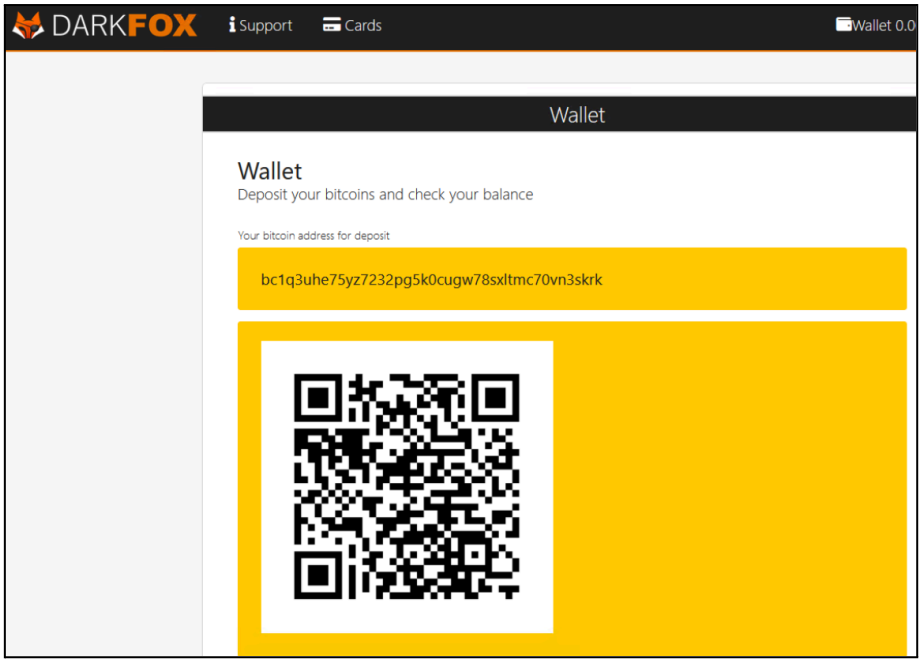


Figure 19 - A QR code on a darknet criminal market wallet to transfer cryptocurrencies (Source: Darkfox)

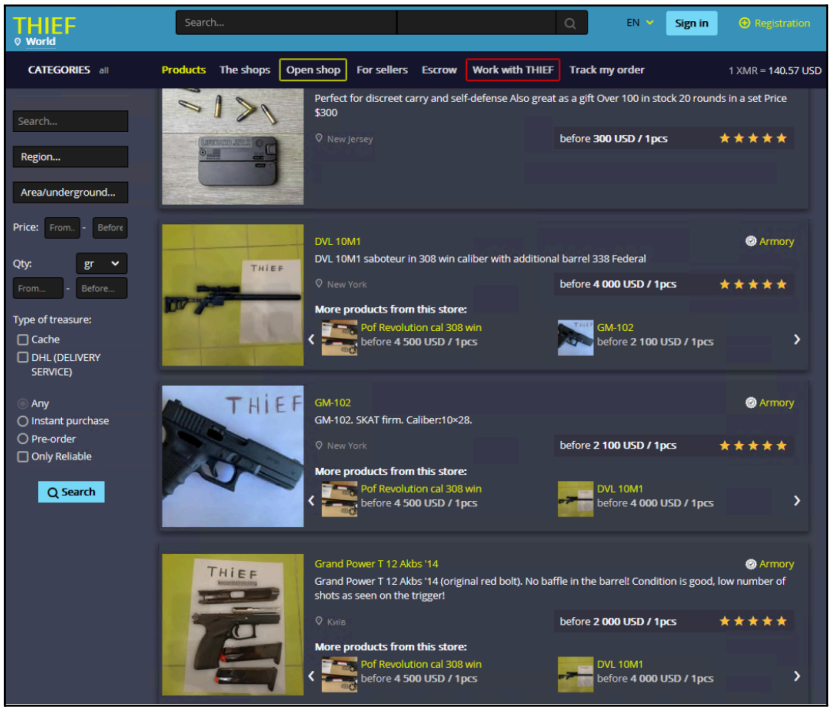


Figure 20 - Example of a darknet criminal weapons market (Source: Thief)

4.1.4 Encrypted Messaging Applications

For many years, encrypted messaging apps have become essential platforms for cybercriminals. From WhatsApp to Telegram, WeChat, TOX, Signal, Threema, or Jabber, these platforms allow cybercriminals to communicate with each other, sell illegal items, and create groups. They are an extension of the classic darknet (TOR or I2P) because they are easier to use and designed for smartphones, making them more flexible. Telegram has gained the most popularity among cybercriminals over the past decade of all these applications. Although its servers are spread across the globe, Telegram's development team is based in the United Arab Emirates, the parent company, Telegram Group Inc., is registered in the British Virgin Islands, and the legal representative for data protection law is Telegram U.K. Holdings Ltd, a company based in the United Kingdom. Its popularity can be attributed to several factors. The application can be used on smartphones and computers. The application provides an end-to-end encryption service and hides the phone number used in the application to delete messages (Figures 21 and 22). This application allows features such as secret chat mode to send secure messages with an automatic deletion feature after a few seconds or minutes. Additionally, Telegram enables the creation of different groups and channels malicious actors use to promote and sell illegal items or services, distribute hacked databases, and recruit people for illicit activities (Figure 23).

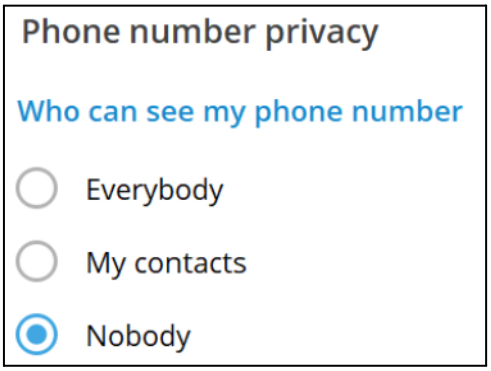


Figure 21- Telegram phone number privacy settings

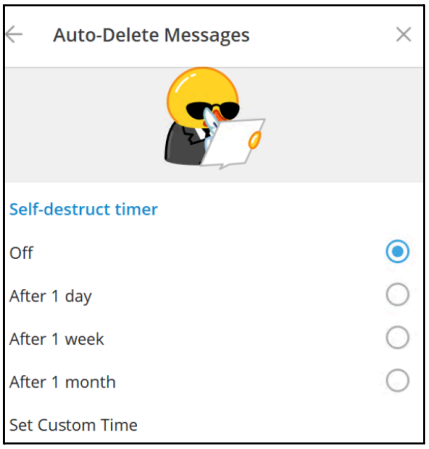


Figure 22 - Telegram Auto-Delete Messages settings

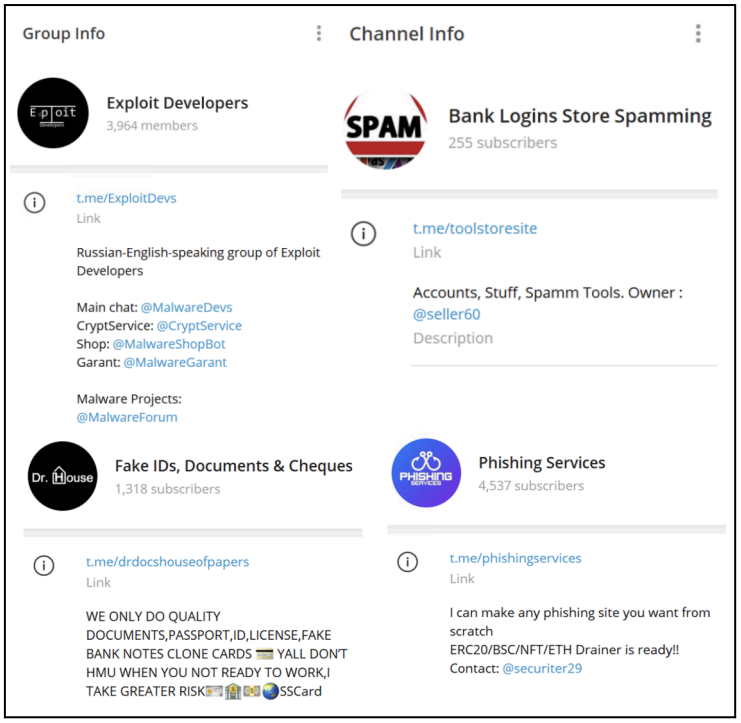


Figure 23 - Examples of different Telegram groups offering illegal items or services

4.2 Cybercrime Organizational Structure:

Much like legitimate enterprises, cybercriminal organizations often mirror the operational frameworks of the corporate world. They typically feature a well-defined hierarchy, clearly assigned roles, and an established chain of command. At the apex of this structure sits a leader or network coordinator, responsible for strategizing and overseeing operations, whether those involve cyberattacks, financial fraud, or illicit trafficking. This figure directs the group's activities and ensures effective communication and coordination among its members (Figure 24). As a result, these criminal enterprises can often execute complex, large-scale schemes with significant financial returns. While their specific objectives may vary, the underlying organizational structure of cybercrime groups tends to remain strikingly consistent. Though roles can shift slightly depending on the area of criminal activity, the general framework typically follows this pattern:



Figure 24 -Cybercriminal Organizational Structure Diagram

Leadership and Strategic Planners

- **Roles**: Organization leaders, strategists, and financiers.
- **Responsibilities:**
    - Setting goals and targets for the organization.
    - Funding operations, often through investments in tools or services.
    - Negotiating partnerships or alliances with other criminal groups.
    - Maintaining high-level anonymity to evade law enforcement.

Developers and Technical Specialists

- **Roles:** Software developers, malware creators, and tool engineers.
- **Responsibilities:**
    - Creating malware (e.g., ransomware, trojans, spyware).
    - Designing hacking tools, exploits, and frameworks.
    - Updating and maintaining systems to bypass security measures.
    - Innovating to keep up with cybersecurity defenses.

Cyber Operators (Hackers)

- **Roles:** Hackers, penetration testers, and system operators.
- **Responsibilities:**
    - Executing attacks, such as phishing campaigns, system intrusions, and data breaches.
    - Gaining unauthorized access to networks and systems.
    - Managing botnets or other compromised systems.

Analysts and Data Handlers

- **Roles:** Data miners, analysts, and data brokers.
- **Responsibilities:**
    - Sorting and analyzing stolen data.
    - Identifying valuable assets, such as credit card details or intellectual property.
    - Packaging and selling stolen information on the dark web.

Money Launderers

- **Roles:** Financial operatives, "money mules," and cryptocurrency experts.
- **Responsibilities:**
    - Moving and converting illicit earnings to legitimate funds.
    - Using cryptocurrencies, shell companies, or online payment systems to obscure transactions.
    - Establishing complex financial networks to avoid detection.

Recruiters

- **Roles:** Talent scouts, social engineers, and human resource specialists.
- **Responsibilities:**
    - Recruiting skilled individuals for various roles.
    - Targeting potential operatives through forums, dark web platforms, or even legitimate job postings.
    - Maintaining connections with freelancers or smaller criminal groups.

Affiliates and Partners

- **Roles:** Contracted operators or external service providers.
- **Responsibilities:**
    - Participating in "as-a-service" operations, such as Ransomware-as-a-Service (RaaS).
    - Renting out infrastructure (e.g., bulletproof hosting or botnets).
    - Collaborating with other groups for large-scale operations.

Technical and Support Staff

- **Roles:** IT support, logistics, and translators.
- **Responsibilities:**
    - Providing technical support for tools or operations.
    - Managing communications and logistics.

4.3 Cybercriminal's Modus Operandi and Operations

4.3.1 Open Source Intelligence

Open Source Intelligence (OSINT) has long served as a valuable asset not just for investigators and analysts, but also for cybercriminals. In today's hyper-connected world, most individuals leave behind a digital footprint composed of various personal and technical data points: phone numbers, email addresses, home addresses, IP addresses, public records, and countless other pieces of information, whether shared knowingly or unintentionally. To cybercriminals, this scattered data represents a digital gold mine, ripe for exploitation in schemes ranging from identity theft to targeted cyberattacks. The proliferation of free and easily accessible OSINT tools has only lowered the barrier to entry. With minimal effort, anyone can gather detailed intelligence on individuals, networks, or entire organizations. Tools such as Shodan, Maltego, ContactOut, RocketReach, TheHarvester, OSINT Framework, SpiderFoot, Google Dorks, Recon-ng, Censys, WHOIS Lookup, BuiltWith, DNSDumpster, Have I Been Pwned, FOCA, and Nmap (Figures 25, 26, 27 and 28) are frequently used in both legitimate research and malicious reconnaissance. Their effectiveness and the sheer volume of data they can uncover makes them indispensable in the modern cyber threat landscape.

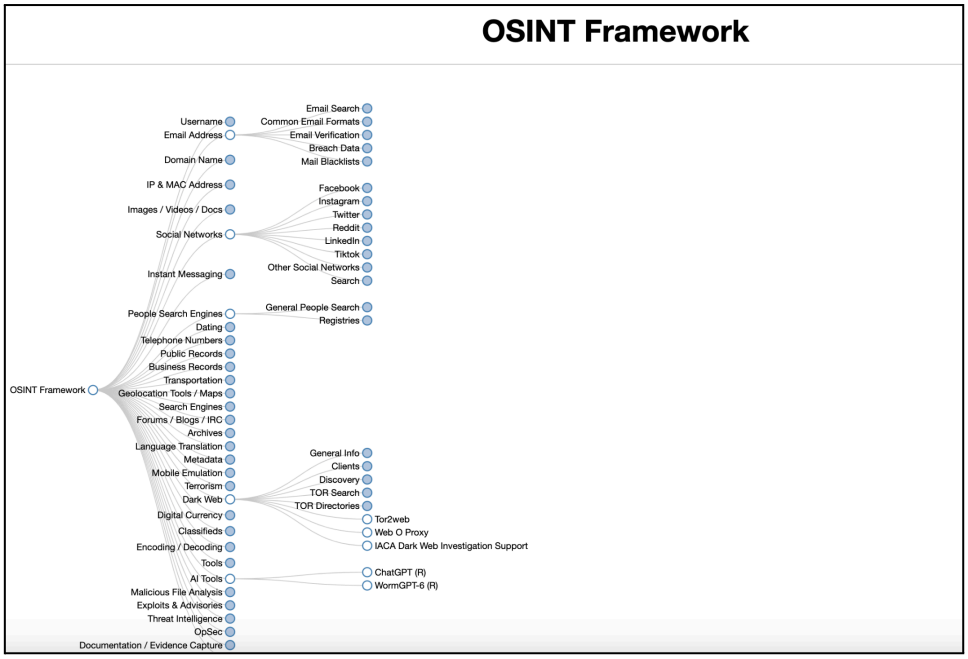


Figure 25 - OSINT Framework repository

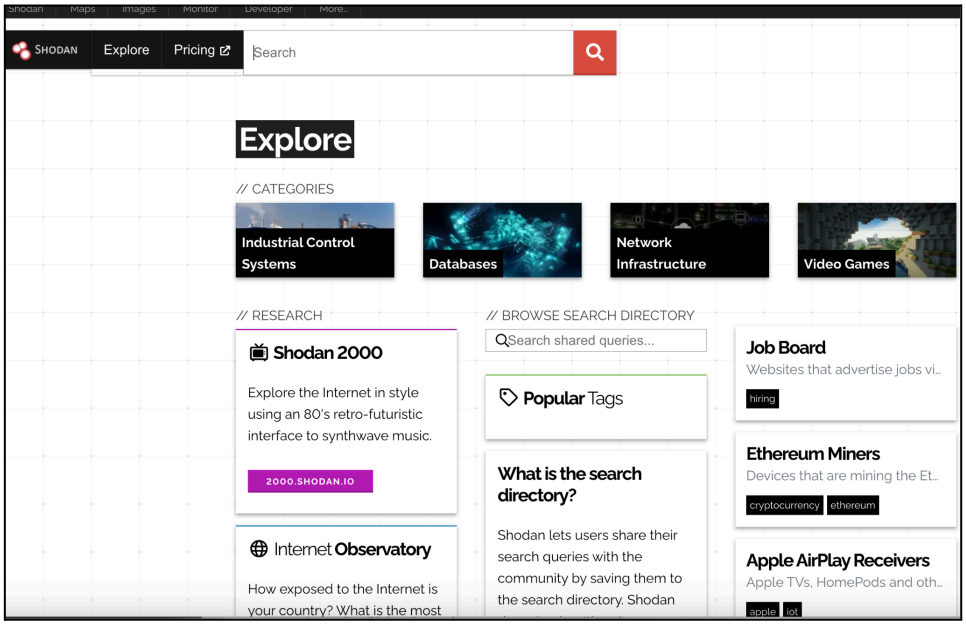


Figure 26 - Shodan IoT search engine

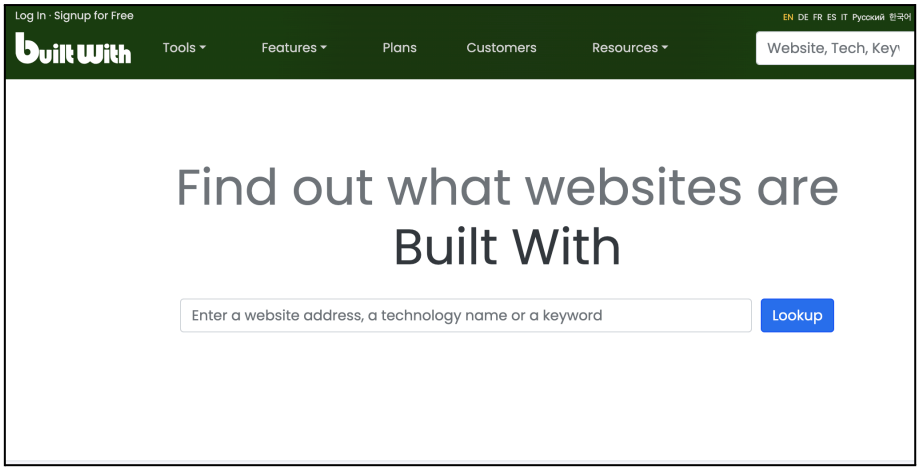


Figure 27 - Built with technology discovery

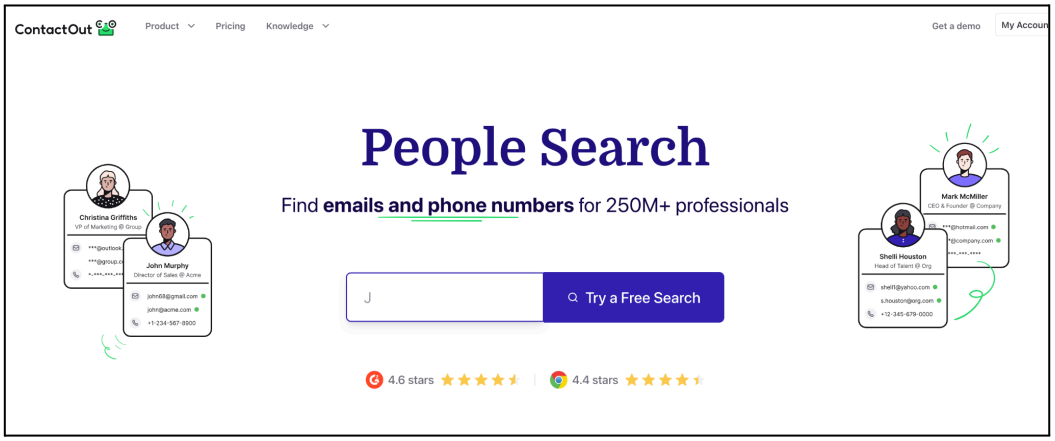


Figure 28 - Contactout people search engine

4.3.2 Social Engineering

Social engineering is one of the threat actors' most well-known techniques to exploit human vulnerabilities. It refers to a wide range of malicious activities carried out through human interactions, including using psychological manipulation to trick users into making security errors or disclosing sensitive information. Social engineering attacks usually involve the following stages:

Collection: This first step typically involves collecting strategic and technical information about the target, such as key people, potential entry points, and security weaknesses.

Approach: This first step involves establishing a voice or written contact with the victim and building a trusted relationship.

Manipulation: This step is a logical continuation of the previous one. Once the trusted relationship has been established and the victim's weaknesses have been detected, the threat actor can psychologically manipulate the victim to obtain what he wishes to get from him.

Disengagement: This last step implies that once the threat actor has obtained the information or actions carried out by the victim in his favor, he stops being in touch with the victim in the most natural way possible, depending on the context and the cover story created.

Psychological manipulation is the key to social engineering success. To carry out their attacks, the most experienced threat actors often study human behavior in cyberspace. They exploit human weaknesses by relying, among other things, on the victims' lack of confidence and their poor or weak knowledge of the cyber environment. Indeed, in the same way that some people feel vulnerable on board a plane because they do not control the environment, the same phenomenon can be observed in cyberspace. Cyberspace is a vast ocean of devices, connections, systems, applications, and actors that is difficult for many people to understand and control. Suppose that humans have more or less succeeded in getting used to cyberspace and its codes (websites, applications, QR codes, 2FA, cookies, etc…); nonetheless, they need to be better informed of the risks and threats incurred. This phenomenon is even more marked among seniors who have not been able to adapt to this new world. Psychological manipulation of the victim can be carried out based on the following principles.

Emotions: Emotional manipulation generally gives the threat actor a strategic advantage when interacting with their victim. When in a heightened emotional state, the victim is much more likely to take irrational or risky actions without realizing it. Threat actors generally use the following emotions to convince their victims: fear, curiosity, excitement, guilt, anger, and sadness.

Emergency: Urgent situations or requests are another reliable tool in a threat actor’s arsenal. A victim can compromise themselves under the cover of a serious problem that requires immediate action.

Confidence: Confidence and credibility are essential during a social engineering attack. The threat actor generally does in-depth research on his victim, allowing him to create a story that is easy to believe and unlikely to arouse suspicion.

Besides these types of manipulation, threat actors can also use more direct methods to access a network or an organization's computer, such as frequenting the public restaurant or rest area of a large office building or replacing the free Wi-Fi network by impersonating it to create a honeypot to collect information about users.

Email and SMS phishing are threat actors' most popular and effective social engineering techniques. The creators of phishing campaigns generally seek to play on factors of importance, urgency, security, curiosity, or fear among victims. Threat actors pose as trusted institutions or individuals to trick their victims into revealing sensitive information, clicking links to malicious websites, or opening attachments containing malware. To lend credibility to their actions, many threat actors include false secure connection signals to trick the victim into believing that the site where they enter their data is safe (Figure 29).

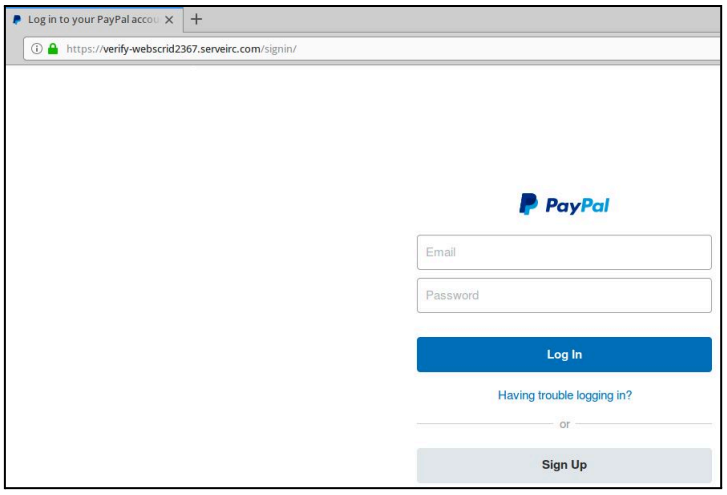


Figure 29 - A phishing page that uses https:// and has the green padlock.

There are several types of phishing attacks, but the most popular are the following:

Email phishing is the most traditional form, using an email to urge you to reply or follow up by other means. Web links, phone numbers, or malware attachments can be used (Figure30). This type of campaign can target a specific category of people (customers of a company or subscribers to a service) or a wider audience with a certain percentage of success on large volumes of email sending.

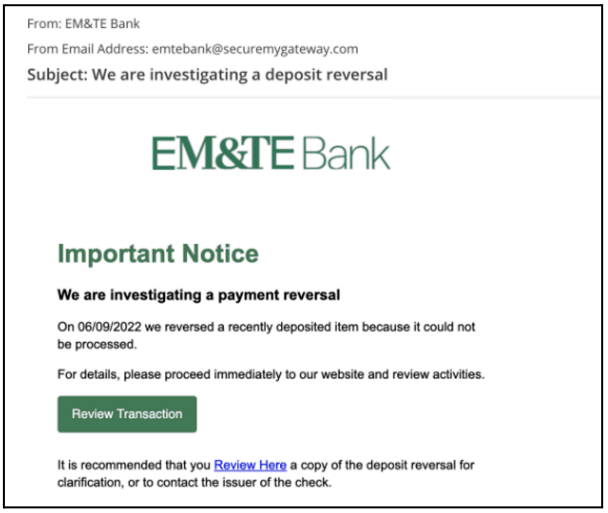


Figure 30 - Bank account verification phishing email example (Source: Keepnet Labs)

SMS phishing (Smishing) is done via text or instant messaging. Typically, threat actors distribute links to redirect to a malicious website or download malicious software stealthily. The emergence of smishing as a tactic results directly from employees using smartphones to access both their text messages and corporate emails (Figure 31). As with email phishing, threat actors generally obtain lists of telephone numbers from hacked customer databases to target a category of people.

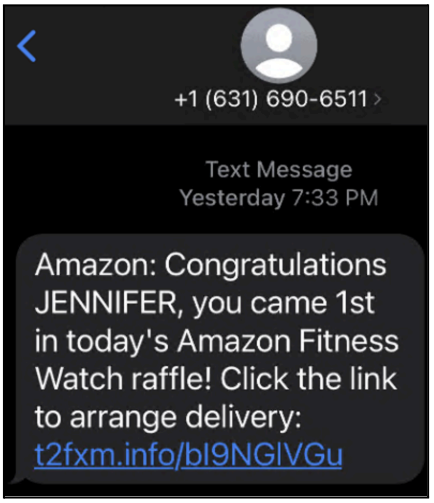
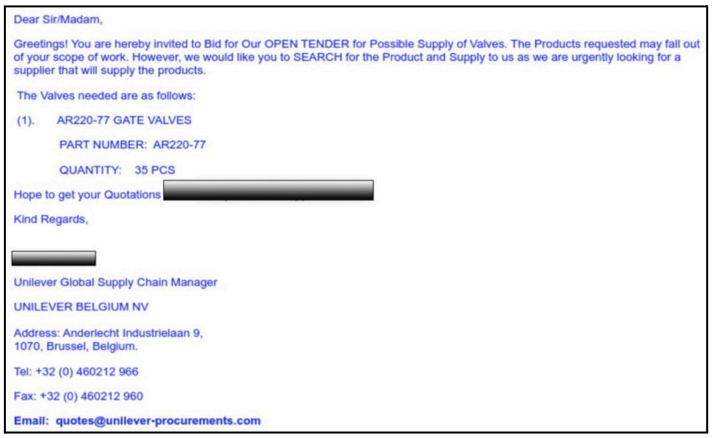


Figure 31- Amazon SMS phishing example (Source: SafetyDetectives)

Business email compromise (BEC) is one of the most financially damaging online social engineering techniques. It exploits the fact that everyone relies on email to conduct their activities, both personal and professional. In a BEC scam, scammers typically send an email from someone within an organization by spoofing their email address and sending what may be considered a legitimate request addressed to a victim within the same organization or being a customer, supplier, or financial partner (Figure 32).


Dear Sir/Madam,

Greetings! You are hereby invited to Bid for Our OPEN TENDER for Possible Supply of Valves. The Products requested may fall out of your scope of work. However, we would like you to SEARCH for the Product and Supply to us as we are urgently looking for a supplier that will supply the products.

The Valves needed are as follows:

(1). AR220-77 GATE VALVES

PART NUMBER: AR220-77

QUANTITY: 35 PCS

Hope to get your Quotations [redacted]

Kind Regards,

[redacted]

Unilever Global Supply Chain Manager

UNILEVER BELGIUM NV

Address: Anderlecht Industrielaan 9,
1070, Brussel, Belgium.

Tel: +32 (0) 460212 966

Fax: +32 (0) 460212 960

Email: quotes@unilever-procurements.com

Figure 32 - A BEC email targeting a multinational manufacturing organization with email impersonation from a third-party vendor. (Source: Fortra PhishLabs)

Quishing (QR code phishing) is a technique where hackers embed malicious links or files in QR codes to evade detection. The threat can bypass email filters that lack QR code detection or reading capabilities. Unlike emails containing a visible link or attachment, it can also make it more challenging for users to diagnose a threat (Figure 33).

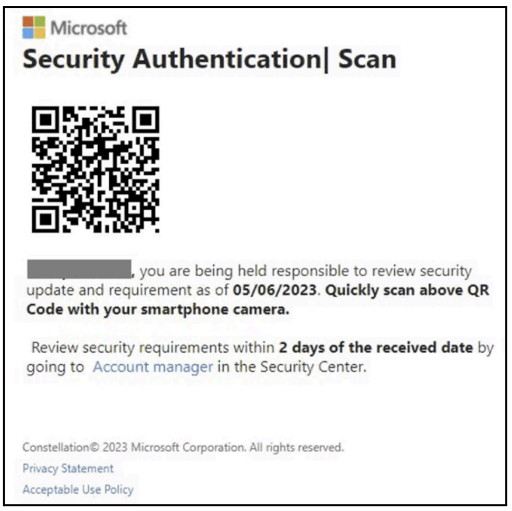


Figure 33 - Microsoft 365 Phishing email example (Source: Vade)

Voice phishing (Vishing) plays on human weakness and psychological manipulation. While classic phishing or smishing can be identified through careful review of the inbound message, threat actors use vishing because of the difficulty of the challenge it poses to the victim to discern the legitimacy of the caller. Vishing specialists often pose as people from customer support, IT, or financial services. They then seek to contact target people and try to extort them. This technique requires a certain amount of self-confidence on the part of the threatening actor because, at some point, he is supposed to be in vocal contact with the victim (Figure 34).

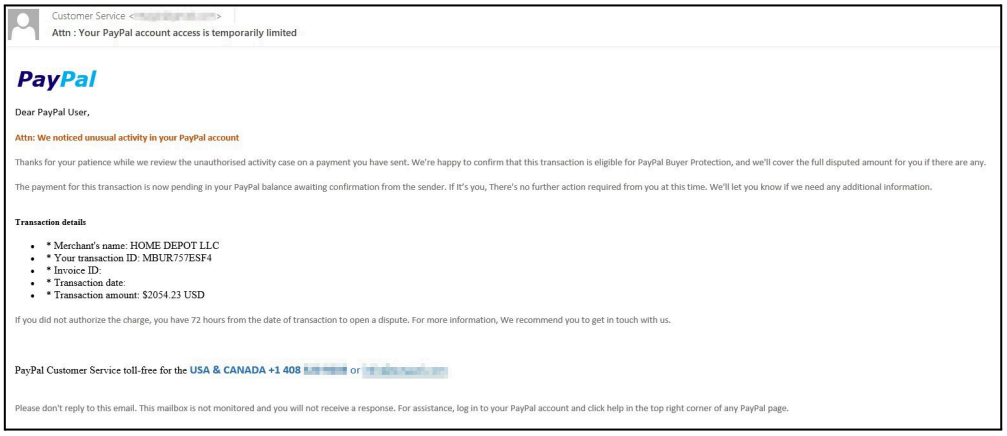


Figure 34 - Fake PayPal notification regarding order cancellation with emergency contact support

Many threat actors offer services or seek to recruit fishing specialists on cybercriminal platforms (Figures 35 and 36).



Figure 35 - A threat actor looking to hire social engineer specialists for calls on a cybercrime forum.



Figure 36 - Professional social engineering service on a cybercrime forum

Pretexting is a social engineering attack in which a scammer invents a pretext or fabricated scenario, usually posing as a person from a public institution such as a tax authority, to trick a victim into providing sensitive personal or financial information. , such as their social security number. In this type of attack, a threat actor can also physically access your data by posing as a supplier, delivery person, or contractor to gain the trust of your staff (Figure 37).

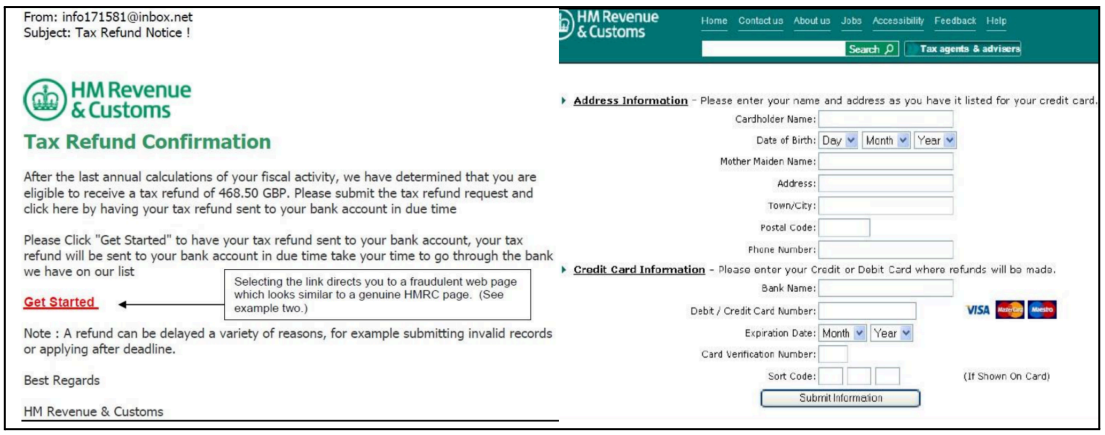


Figure 37- Fake UK Revenue and Customs phishing pages to collect financial data

Spear phishing uses personalized information to target particular users. This information is collected through different means (leaked databases, open source, etc.). The attacks target high-value targets such as celebrities, senior executives, and high-ranking government officials. To make themselves credible, they generally pose as a known institution, a person from the same company, or the same public entity (Figure 38).

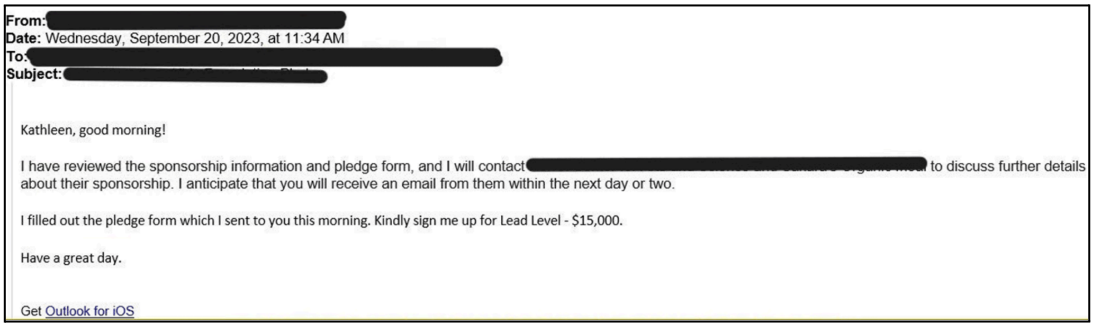


Figure 38 - Spear Email phishing example (Source: Vade)

Angler phishing is performed on social media. An attacker imitates a trusted company's customer service team. They intercept your communications with a brand to hijack and divert your conversation into private messages, where they then advance the attack (Figure 39).

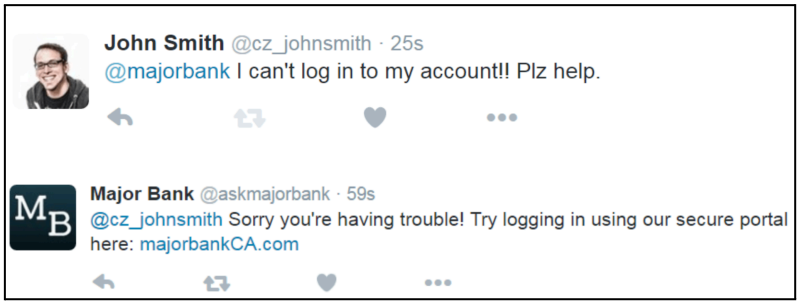


Figure 39 - Angler phishing example on X social network (Source: Proofpoint)

Search engine phishing involves indexing links to fake websites at the top of search results. These may be paid ads or legitimate optimization methods for manipulating search rankings (Figure 40).

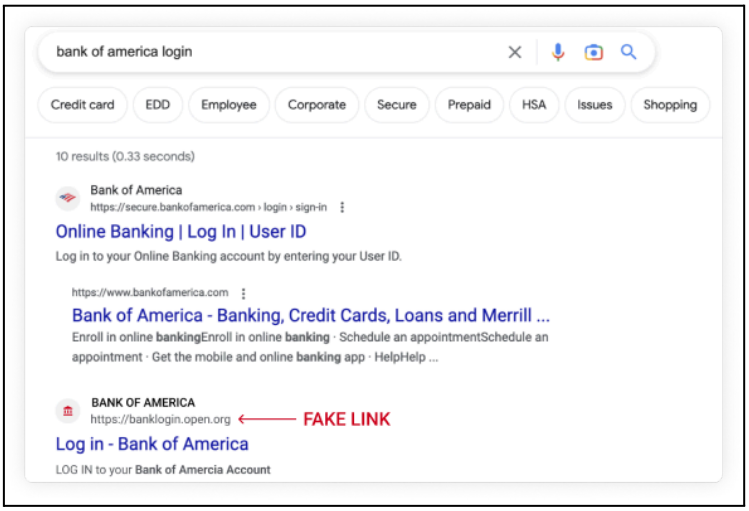


Figure 40 - Search engine phishing example (Source: Keeper)

In-session phishing interrupts everyday web browsing with fake login pop-ups for pages you're visiting. The baiting attack involves exploiting victims' curiosity to trick them into exposing their data. Typically, threat actors lure and manipulate their victims with the help of tempting advertisements and free offers. The attack usually involves infecting the victim with malware. One of the most popular hacking methods is attaching email attachments containing details about a free offer or fraudulent freeware. Another popular form of baiting is using physical media to spread malware. Some threat actors use USB drives to infect them with malware, often leaving them statically in areas where potential victims are sure to see them and are lured by curiosity to see what the connector contains on a personal or professional computer. Social engineering, phishing, vulnerability exploitation, and supply chain attacks are among the most popular attack vectors cybercriminals use to penetrate networks and systems of public and private organizations.

4.3.3 Virtual HUMINT

Virtual HUMINT (Human Intelligence) combines traditional HUMINT methodologies with modern IT tools and digital skills to identify, recruit, manipulate, and gather intelligence on individuals or targets operating in online environments. This discipline employs a range of techniques, including social engineering, negotiation strategies, and natural language processing (NLP), as previously discussed. Practitioners of virtual HUMINT must possess a strong understanding of human psychology, intelligence operations, and the dynamics of cyberspace. Threat actors across various domains such as terrorism, cybercrime, espionage, hacking, and fraud frequently use virtual HUMINT to conduct operations online, leveraging the intricacies of human interaction through digital platforms. Ultimately, the effectiveness of a virtual HUMINT operation depends heavily on the human element.

When a threat actor initiates an undercover online operation, they typically begin with baseline intelligence about the target and a clearly defined objective. Contact with the target can be established in seconds, but success hinges on crafting a credible and convincing identity or *legend*. The creation of such a persona varies depending on the operation's nature, but it must always be believable enough to deceive the intended victim. Cyber operations, whether focused on criminal activity, espionage, influence campaigns, or terrorism, often unfold through social media platforms like Facebook, LinkedIn, and Instagram, or via encrypted messaging apps such as WhatsApp and Telegram. As noted earlier, although most people are familiar with social media, few are adept at recognizing suspicious or entirely fabricated profiles. Malicious actors exploit this gap by creating fake personas tailored to their operational goals. Some even impersonate senior personnel within legitimate organizations to boost their credibility and increase the likelihood of successful engagement (Figure 41).

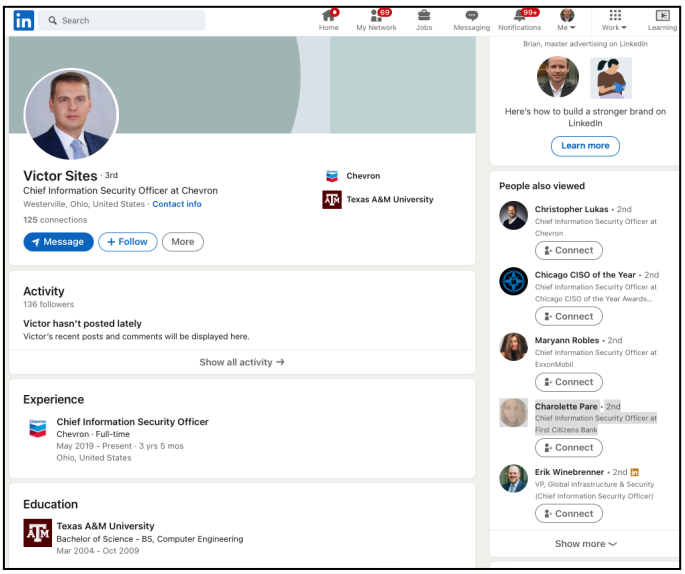


Figure 41 - A fake LinkedIn profile of a person impersonating the position of CISO at Chevron (Source: Brian Krebs).

This tactic is effective on unsuspecting individuals who fail to thoroughly verify someone's identity, especially when they see shared connections. Some threat actors even go as far as fully impersonating real individuals. According to the cybersecurity firm Mandiant, hackers linked to the North Korean government have engaged in cyber espionage by replicating CVs and profiles from major job platforms like LinkedIn and Indeed. This was part of a calculated effort to secure positions at cryptocurrency companies. Once these fake profiles are crafted with varying professionalism levels, threat actors typically reach out to their targets under a seemingly legitimate and well-structured pretext (Figure 42).

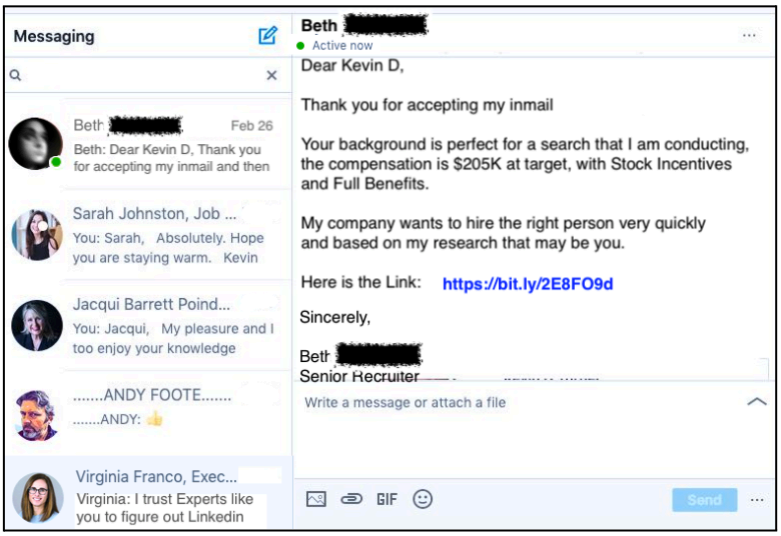


Figure 42 - A Fake Job Offers Spread Malware via LinkedIn Messaging, Invite, & InMail.(Source: LinkedIn)

While threat actors often rely on naive victims or unfamiliar with emerging technologies, even individuals well-versed in online safety can fall prey to deception. In 2022, according to antivirus firm BitDefender, a British woman described as a technology expert with strong awareness of online scams was tricked into transferring nearly £16,000 (about $21,000) of her savings to fraudsters impersonating her daughter on WhatsApp (Figure 43). She stated:

"I received a text message from what I presumed was my daughter, Sam, asking me to delete the old phone number as she'd been given a new number. It went on after a couple of lines of text to ask me if I would make a transaction for her, which I agreed to if she sent me the sort code, the payee's details, and the account number. I presumed it was my daughter, and I thought, well, because of the situation, I could do that. I started suspecting something was wrong when Sam didn't reply to say good night."



Figure 43 - WhatsApp conversation between a British woman and a scammer pretending to be her daughter.

The effectiveness of a Virtual HUMINT operation often hinges on the attacker's ability to tailor their communication to the cultural and linguistic context of the target. Depending on the objective, whether industrial espionage, political manipulation, or financial fraud, threat actors craft messages designed to appear credible. The professionalism of the attacker is often revealed in their language, tone, and syntax. Poor grammar, awkward phrasing, obvious machine translation, or inappropriate symbols and emojis can immediately raise suspicion. In contrast, the most successful Virtual HUMINT campaigns are executed by actors who demonstrate fluency not only in the target's language but also in regional slang, idiomatic expressions, and cultural nuances factors that vary significantly even among countries sharing the same official language (e.g., US vs. UK, Spain vs. Mexico, France vs. Belgium, or across various Arab nations). Mastery of these subtleties often distinguishes a convincing deception from an exposed attempt.

4.3.4 Malware and Exploits

Malware and exploits are key tools cybercriminals use to carry out their attacks. These tools are crucial for gaining unauthorized access to systems, stealing sensitive information, or causing disruption. Malware, short for malicious software, refers to any program designed to damage or steal data from computers or networks. It includes viruses, worms, trojans, ransomware, and spyware, each with its harmful purpose. On the other hand, exploitation is specialized programs or actions that take advantage of weaknesses or vulnerabilities in software or hardware. These vulnerabilities can be flaws the developers haven't yet fixed, making them prime targets for cybercriminals. Cybercriminals often spend a lot of time searching for these weaknesses, called "zero-day" vulnerabilities, which are not yet known to the software makers. Once they find one, they can create an exploit to

break into systems and carry out their attacks. These attacks can range from stealing personal data to locking systems and demanding money (ransomware), or simply causing chaos in a network. Malware and exploits are also traded in underground online markets, where criminals buy and sell these dangerous tools. This shows just how important they are in the world of cybercrime. Understanding how these tools work and how they are used is crucial to strengthening defenses against cyber threats.

Ransomware

Among all forms of malware, ransomware has emerged as one of the most pervasive and destructive threats of the past decade. Its evolution has been marked by increasingly sophisticated tactics and diverse attack vectors. Today, ransomware represents one of the most formidable challenges in cybercrime. The financial incentives for attackers are considerable, with ransom demands often far exceeding the cost of developing and deploying the malware. In recent years, many ransomware operators have adopted a strategy known as double extortion. This method involves encrypting the victim's systems and data and exfiltrating sensitive internal information beforehand. Cybercriminals then leverage this stolen data to apply additional pressure, threatening to publish or sell it if the ransom is not paid, often escalating their demands by emphasizing the value or sensitivity of the compromised material. This dual-threat tactic not only increases the potential financial gain but also amplifies the psychological stress on victims, who face both operational paralysis and reputational damage. The rise of Ransomware-as-a-Service (RaaS) has further fueled the proliferation of these attacks. By offering ready-made ransomware kits on the dark web, skilled developers have enabled even non-expert cybercriminals to launch effective campaigns, greatly expanding the threat landscape (Figure 44). Numerous websites now track and list ransomware incidents, including the names of victims, offering insight into the evolving patterns of these attacks across countries, industries, and periods (Figures 45 and 46). Ransomware is expected to remain a dominant tool in the cybercriminal arsenal. Its methods will likely continue to evolve, becoming more advanced and better adapted to bypass modern cybersecurity defenses.

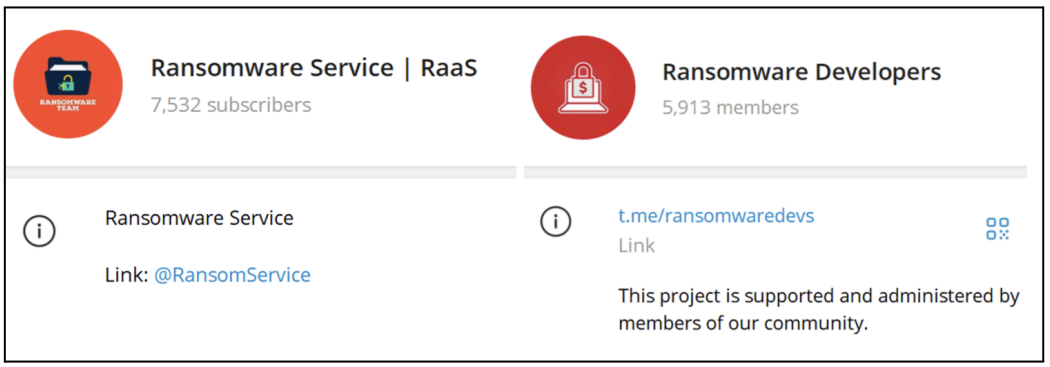


Figure 44 - Ransomware services on Telegram

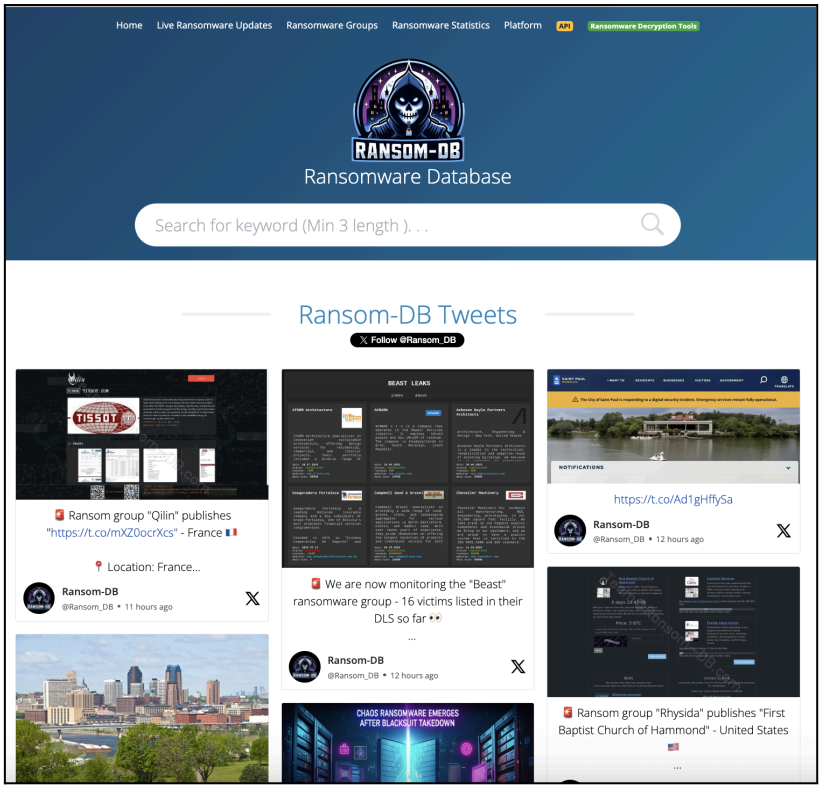


Figure 45 - A live ransomware tracker website (Source: ransomware.DB)

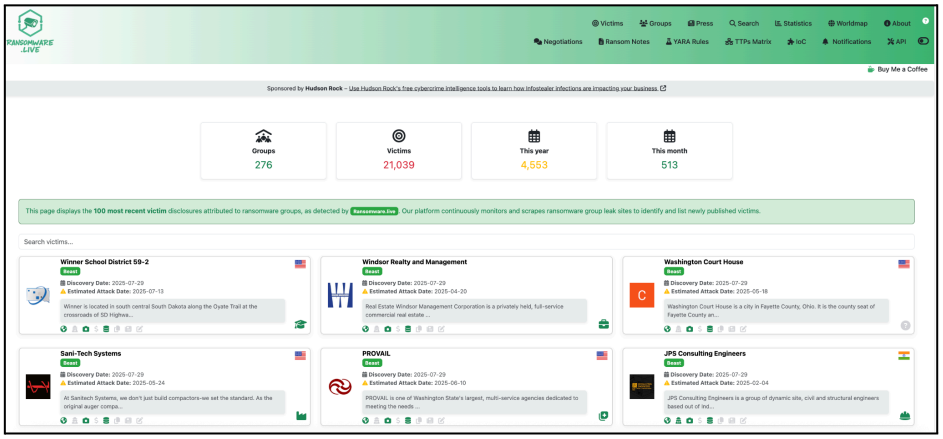


Figure 46 - A live ransomware tracker website (Source: ransomware Live)

Data Collection Malware

In the evolving landscape of cyber threats, **data collection malware** has emerged as one of the most persistent and dangerous tools leveraged by cybercriminals. This category of malicious software is specifically engineered to infiltrate systems, extract sensitive information, and transmit that data to unauthorized third parties—typically without the knowledge or consent of the victim. As our reliance on digital services increases, and with it the volume of personal, financial, and corporate information stored online, the incentive for cybercriminals to deploy such malware has grown exponentially. Data collection malware operates silently in the background, harvesting valuable data such as login credentials, credit card numbers, health records, business communications, and proprietary documents. Once acquired, this information is often sold on underground marketplaces like the dark web, used directly for financial fraud, or exploited in targeted cyber-espionage campaigns. Over the years, these threats have evolved from relatively unsophisticated scripts to highly complex, adaptive programs capable of evading detection by traditional antivirus tools. Many variants can monitor user activity in real time, intercept communications, or even exfiltrate data from secure environments through covert channels. Commonly used in criminal enterprises and state-sponsored attacks, data collection malware is a versatile tool that plays a central role in many malicious campaigns. Understanding its characteristics, attack vectors, and functional mechanisms is essential for any individual, organization, or government seeking to defend against modern cyber threats. As cybercriminal techniques continue to advance, data collection malware is expected to remain a prominent threat, making proactive detection, user education, and robust security architecture more critical.

Key Characteristics of Data Collection Malware

- **Stealthy Operation:**
  - Operates covertly to avoid detection by the user or security software.
  - Employs obfuscation techniques like encryption or polymorphism to evade antivirus systems.
- **Targeted Data Gathering:**
  - It focuses on data types such as credentials, financial information, browsing history, and system configurations.
  - Some are designed for mass collection, while others target specific entities or industries.
- **Persistence Mechanisms:**
  - Installs itself in ways that ensure it survives system reboots or software updates.
  - Creating scheduled tasks.
  - It can use techniques like rootkits or registry modification to keep it hidden.
- **Exfiltration Capabilities:**
  - Uses secure channels (e.g., encrypted communications) to send stolen data to a remote command-and-control (C2) server.

    - Using legitimate protocols like HTTPS, DNS tunneling, or file-sharing services to blend in with regular traffic.
- **Versatility:**
    - Often modular, allowing attackers to add or change functionality after deployment.
    - It can adapt based on the environment it is deployed in.
- **Delivery Mechanisms:**
    - Spread through phishing emails, malicious websites, infected software, USB drives, or network vulnerabilities.

Functions and Work of Data Collection Malware

- **Data Harvesting:**
    - It collects sensitive user information such as usernames, passwords, email addresses, credit card numbers, and personal identification numbers.
    - Targets system information, including logs, clipboard data, and screenshots.
- **Credential Stealing:**
    - Exploits browser vulnerabilities or uses keyloggers to capture credentials entered into websites or applications.
- **Network Monitoring:**
    - Monitors and records network traffic to intercept sensitive data being transmitted.
- **Database or File Extraction:**
    - Targets local or network databases to exfiltrate customer data, intellectual property, or financial records.
    - May search for specific file types or keywords.
- **Keylogging:**
    - Records keystrokes to capture typed information like passwords, search queries, or chat messages.
- **Clipboard Monitoring:**
    - Monitors the clipboard to capture copied information, such as credit card details or cryptocurrency wallet addresses.
- **Exfiltration of Data:**
    - Compresses and encrypts collected data before transmitting it to a remote server controlled by the attacker.
- **Screen Capture and Webcam Recording:**
    - Takes screenshots or records video/audio from a device to gather additional sensitive information.
- **Browser and Email Data Theft:**
    - Extracts saved browser credentials, browsing history, or email contents.

On the dark web, many cybercriminals offer to sell or recruit people to develop malware projects such as RAT, stealer, and others. The price of this malware generally varies depending on the features included (screenshot, form grabber, keylogger...) and the sophistication (AV bypass, encryption...) and can thus range from several hundred to several thousand dollars (Figure 47 and 48)

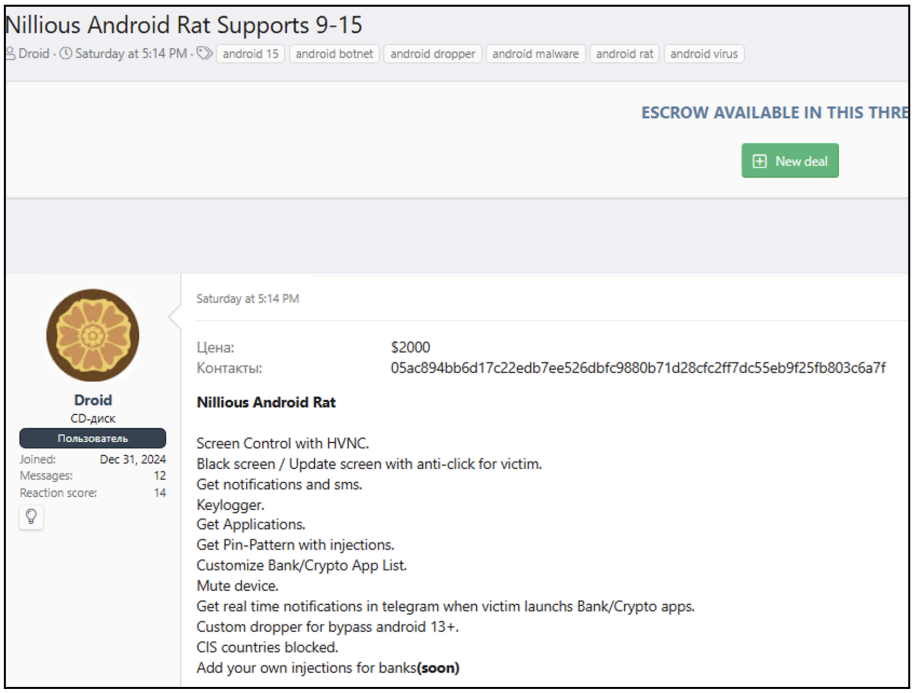


Figure 47 - Android RAT for sale on a cybercrime forum

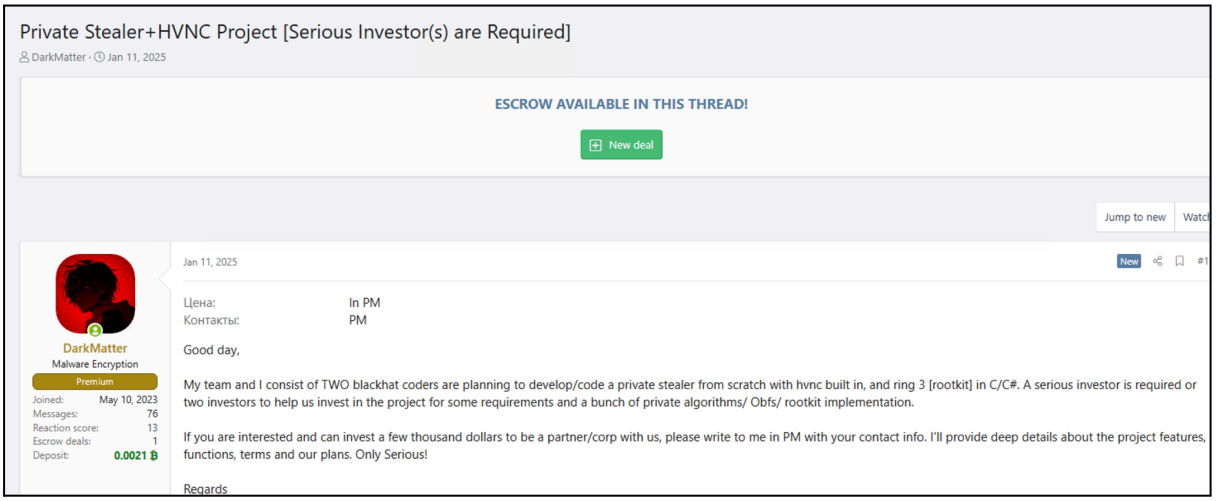


Figure 48 - A cybercriminal offering to join a private stealer development project on a cybercrime forum

4.3.5 Exploits and Vulnerabilities

Developing and exploiting vulnerabilities constitutes a fundamental aspect of the cybercriminal toolkit. Cyberattacks frequently rely on identifying and abusing security flaws, whether these are publicly known vulnerabilities or previously undiscovered "zero-day" exploits. These weaknesses often serve as critical entry points, granting unauthorized access to networks, systems, or devices. Once inside, attackers can exfiltrate data, deploy malware, or escalate their privileges to compromise the environment further.

At the heart of this malicious activity lies the exploit market a thriving, clandestine economy that plays a pivotal role in the broader cybercrime ecosystem. Within this marketplace, cybercriminals and advanced threat actors develop, trade, and sell exploit code and techniques targeting software, hardware, and system-level vulnerabilities. These exploits can range from basic scripts targeting outdated software to sophisticated chains that nation-state actors use. This illicit trade predominantly occurs on the dark web and various underground forums, where anonymity is preserved and transactions are often conducted using cryptocurrencies. The exploit market fuels a continuous cycle of discovery and weaponization, enabling attackers to stay one step ahead of defensive technologies. Below is a closer examination of how exploits are developed, utilized, and monetized within this underground ecosystem:

Development of Exploits

Exploits are frequently developed by highly skilled cybercriminals who possess advanced technical expertise across multiple domains, including reverse engineering, software development, and vulnerability analysis. These individuals have an in-depth understanding of computer systems, programming languages, and security protocols, allowing them to identify and manipulate weaknesses in software or hardware. Their sophisticated knowledge enables them to craft tailored attacks that can bypass traditional security measures, often with the intent of gaining unauthorized access, exfiltrating sensitive data, or disrupting targeted systems.

- **Exploits:**
    - **Zero-Day:** These target vulnerabilities are unknown to the software vendor and are the most valuable in the exploit market.
    - **Known Vulnerabilities**: Older vulnerabilities are often exploited when users fail to update or patch their systems.
    - **Bug Bounties Gone Rogue:** In some cases, legitimate researchers may sell their discoveries on the dark web instead of reporting them to vendors.

Sale of Exploits

Over the past decade, the commercialization and distribution of exploits for software vulnerabilities have grown significantly, becoming a more prominent aspect of cybersecurity. This expansion has been partly driven by the increasing demand for such tools among threat actors, security researchers, and even state-sponsored entities. Despite their growing prevalence, obtaining reliable, high-quality exploits remains a challenge. The market is fragmented, and the quality of available exploits varies greatly. Many of these transactions occur in clandestine online forums and marketplaces, often hosted on the dark web or through encrypted platforms such as Telegram. These underground ecosystems range from loosely organized channels offering low-level, often repackaged exploits to highly exclusive groups dealing in sophisticated, zero-day vulnerabilities. As a result, navigating this shadowy marketplace requires technical expertise and a strong understanding of the credibility and reputation of the sellers involved.

- **Dark Web Forums and Marketplaces:**
    - **Exploits** are sold on specialized dark web forums or marketplaces like exploit shops.
    - **Prices and access** are often controlled via cryptocurrencies for anonymity.
- **Exploit Brokers:** Brokers act as intermediaries between buyers and sellers, connecting those looking to monetize exploits with interested parties, including nation-states.
- **Subscription Models:**
    - **"Exploit-as-a-Service"** offers access to a portfolio of exploits for a recurring fee.
    - **Exploit kits** bundle multiple exploits with user-friendly interfaces, allowing less skilled cybercriminals to launch attacks.
- **Price: The value of an exploit depends on:**
    - **Type of Exploit:** Zero days are the most expensive, ranging from tens of thousands to millions of dollars.
    - **Target System**: Exploits targeting critical systems (e.g., operating systems, IoT devices) or popular platforms (e.g., Windows, iOS, Android) are more valuable.
    - **Ease of Use:** Plug-and-play exploits fetch higher prices due to their accessibility to non-technical users.

Uses of Exploits

- **Financial Fraud:** Exploits are used to steal financial information (e.g., credit card details, online banking credentials).
- **Ransomware:** Deployment: Many ransomware campaigns use exploits to compromise systems and deploy payloads.

- **Botnet Creation:** Exploits infect devices, turning them into part of a botnet for DDoS attacks or other malicious purposes.

Exploit Market Trends

- **Increased Automation:** Many exploit kits now automate attacks, broadening their usability.
- **Focus on IoT and Mobile Devices:** As traditional systems become more secure, attackers increasingly target less protected IoT devices and mobile platforms.
- **Collaboration with Malware Developers:** Exploit developers often collaborate with malware creators to deliver exploits alongside malicious payloads.
- Underground Training: Some forums offer tutorials and training for aspiring exploit developers, expanding the pool of cybercriminals capable of creating and using exploits.

4.3.5 Network Access and Data Breach

As of 2025, exploitable entry points within corporate networks remain among the most critical vulnerabilities in the digital security landscape. Cybercriminals are no longer just targeting personal data or confidential reports; they are now pursuing broader, more strategic assets such as proprietary technologies, operational data, and critical infrastructure controls. While traditional methods of breaching networks through phishing campaigns or malware injections remain active, a more efficient and increasingly popular alternative has emerged: purchasing access to compromised networks (Figures 49 and 50). This practice has created a thriving underground marketplace where initial access brokers (IABs) serve as intermediaries, offering unauthorized access to enterprise environments across every industry. These transactions are commonly conducted on dark web forums and encrypted communication platforms, where access credentials are sold to the highest bidder. Popular access types include Remote Desktop Protocol (RDP), Secure Shell (SSH), Virtual Private Network (VPN), Citrix, cPanel, File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP). The pricing of such access is typically determined by several variables, including the target organization's annual revenue, employee count, the number of endpoints, industry type, and even the strength of its cybersecurity posture.

Recent data from IBM's *2025 Cost of a Data Breach Report* illustrates the escalating financial impact of these intrusions. The average global cost of a data breach has climbed to $5.3 million, an increase of 9% from the previous year and the highest recorded to date. Organizations with fully deployed AI-driven security systems and mature incident response frameworks were able to contain breaches significantly faster and with lower financial impact. However, over 60% of affected companies

reported severe shortages in skilled cybersecurity personnel, a stark 26.2% increase over the previous year, further compounding their exposure and delaying recovery efforts. Looking ahead, this illicit market for network access is expected to become more sophisticated and commercialized. Emerging trends include subscription-based models, tiered access levels, and affiliate networks that mirror legitimate software-as-a-service (SaaS) structures. To counter these developments, businesses must adopt a forward-looking, intelligence-led approach to cybersecurity anchored in zero-trust architectures, real-time threat detection, and continuous employee training. The battle against unauthorized access is no longer just a technical challenge; it is a strategic imperative central to organizational resilience in the digital age.

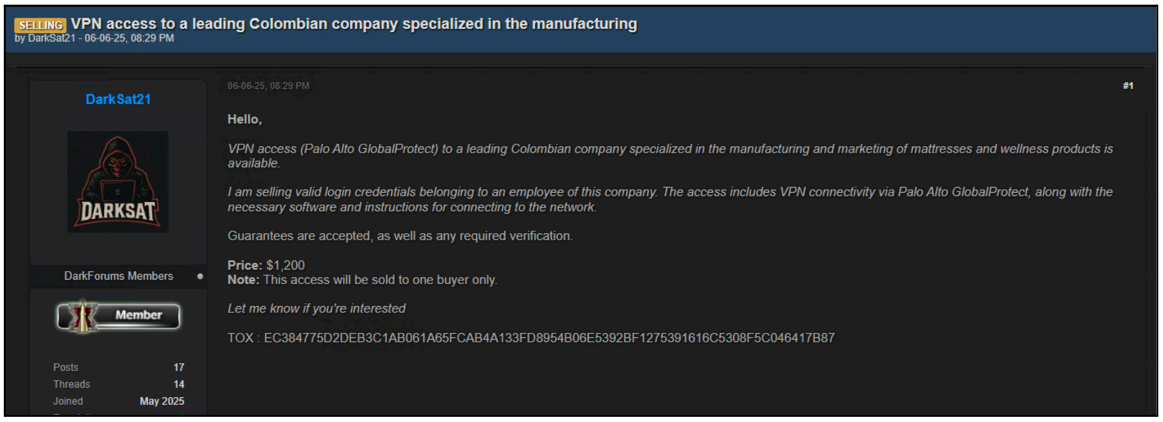


Figure 49 - Network access (VPN) to a Colombian company for sale on cybercrime forum

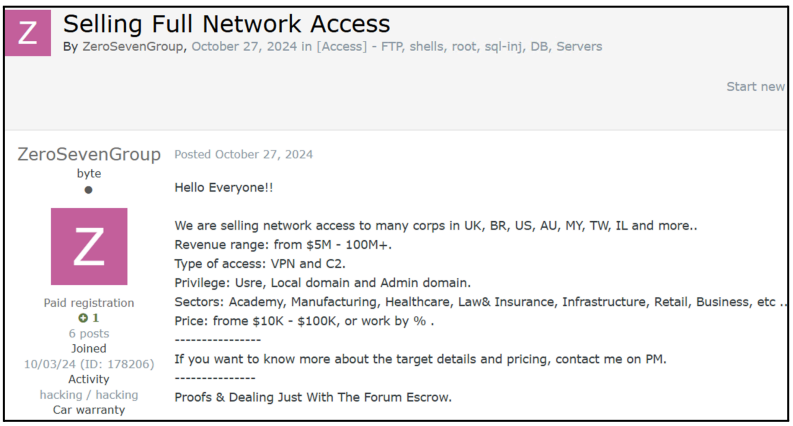


Figure 50 - Network access (VPN and C2) to multiple companies worldwide for sale on a cybercriminal forum

4.4 Cybercriminals' Psychology

Successfully fighting cybercrime requires more than advanced technology and strict legal frameworks; it necessitates a thorough understanding of the psychological drivers behind such criminal behavior. Delving into the mindset of cybercriminals allows for developing more precise, informed, and practical strategies to prevent and respond to cyber threats. A multifaceted combination of personal motivations, cognitive processes, emotional states, and behavioral patterns shapes the psychology of cybercriminals. These psychological elements influence how cybercrimes are conceptualized and executed and how perpetrators rationalize their actions. Factors such as a desire for financial gain, power, recognition, ideological expression, or even revenge often play a critical role in motivating cybercriminal activities. Additionally, traits such as low empathy, high risk tolerance, and a sense of detachment from victims due to the virtual nature of crimes further enable such behavior. By understanding these underlying psychological dimensions, cybersecurity professionals and law enforcement agencies can better anticipate criminal actions, tailor intervention strategies, and strengthen global defense against cybercrime.

4.4.1 Motivations

- **Financial Gain:** The most common driver targeting valuable data, intellectual property, or direct monetary theft.
- **Revenge:** Cyberattacks as a way to harm specific individuals, organizations, or governments.
- **Recognition or Status:** Demonstrating technical skills to earn respect or notoriety in online communities.
- **Thrill-Seeking:** Some cybercriminals are motivated by the challenge and excitement of bypassing security systems.
- **Curiosity:** Young or inexperienced individuals may start as hobbyists exploring systems before transitioning into criminal activities.

Way of Thinking and Cognitive Bias

- **Rationalization:** Many cybercriminals justify their actions by believing that large corporations or governments are worth targeting or will not suffer significant damage.
- **Overconfidence and risk perception**: Some cybercriminals, having high confidence in their skills and the anonymity offered by networks like TOR or using tools like VPNs, tend to underestimate the likelihood of being detected and stopped.
- **Moral disengagement:** They may compartmentalize their actions, dissociating them from ethical, moral, and victim impact concerns.

Behavioral Characteristics

- **Opportunistic Behavior:** Some cybercriminals look for easy-to-use solutions, such as systems with weak security, default credentials, or unpatched vulnerabilities.
- **Adaptability:** They continually learn and evolve their tactics, techniques, and procedures (TTPs) to counter evolving cybersecurity measures.

4.4.2 Psychological Profiles

Some traits are common to cybercriminals:

- **Introversion and isolation:** many operate alone or in small groups and spend much time online.
- **Intelligence:** cybercriminals often have advanced problem-solving and technical skills.
- Lack of empathy: The vast majority of cybercriminals are little concerned with the harm caused to victims and the consequences their actions have on them (financial, psychological, etc.).
- **Ego:** need for validation or the thrill of outwitting systems and demonstrating their capabilities and know-how.

Beyond these typical profiles and characteristics of cybercriminals, there are also cultural factors. Cultural factors significantly influence the psychology and behavior of cybercriminals, shaping their motivations, techniques, and ethical boundaries. These factors include societal values, norms, legal frameworks, and socio-economic conditions. Here's how they manifest:

Motivations Shaped by Socioeconomic Context

- Economic Hardship: In countries with high unemployment or poverty rates, individuals may use cybercrime to achieve financial stability.
- Cultural Acceptance of Illicit Activities: In some cultures, cybercrime might be considered a lesser or acceptable offense, mainly if it targets foreign entities or "wealthy" nations.

Perception of Ethics and Legitimacy

- **Cultural Relativism:** What is deemed unethical in one culture may be seen as clever or innovative in another. For example, hacking into a system might be celebrated as a sign of technical skill in specific communities.
- **Collectivism vs. Individualism:** In collectivist cultures, cybercrime may be rationalized as an act for the greater good, such as targeting governments or corporations seen as exploitative.

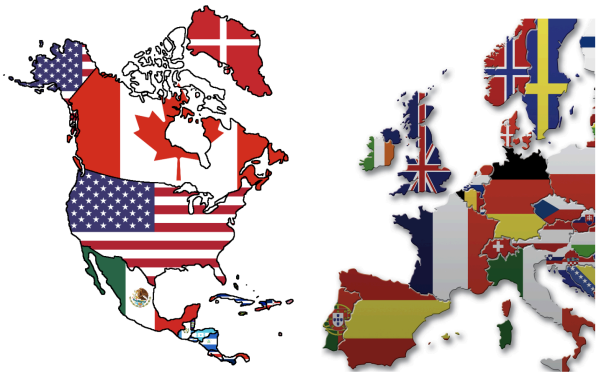
Globalization and Cultural Collaboration

- **Cybercrime Networks:** Cybercriminals often form cross-cultural networks, utilizing differences in laws and enforcement to their advantage. For instance, one group might operate in a country with lax cybersecurity laws while targeting victims elsewhere.
- **Cultural Adaptation:** Cybercriminals tailor their attacks to exploit cultural nuances, such as phishing emails that mimic local linguistic and social customs.

4.5. Geographical Distribution of Cybercrime

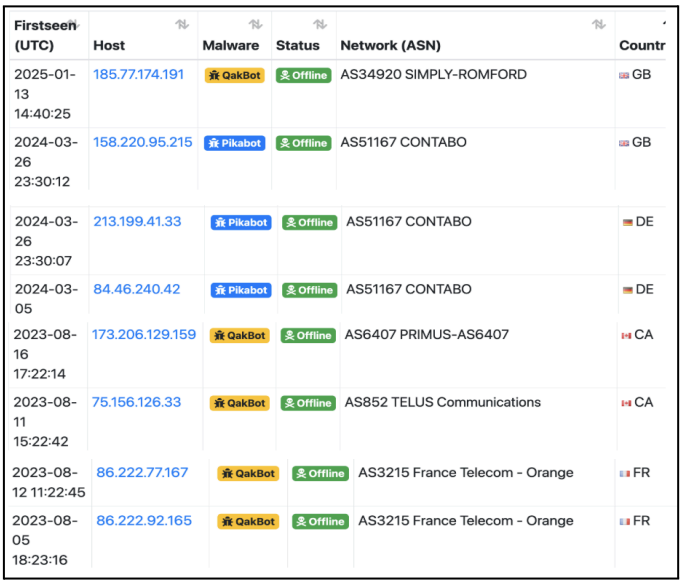
Cybercrime is a global phenomenon, but its patterns and impact are different worldwide. The geographical distribution of cybercrime reflects a complex interplay of technological development, internet penetration, law enforcement capabilities, socioeconomic conditions, and political stability. In some regions, cybercrime thrives due to weak legal frameworks and limited cybersecurity infrastructure, while others face constant threats despite advanced digital defenses. Moreover, regional differences in prevalent cybercrimes, ranging from financial fraud and ransomware to state-sponsored attacks and hacktivism, reveal how local contexts influence the global threat landscape. This section explores these dynamics on a regional basis, offering a comparative analysis of how cybercrime emerges, evolves, and is addressed worldwide.

4.5.1. Western Europe and North American Countries



Cybercrime poses a persistent and evolving threat to North America and Western Europe, which remain prime targets due to their economic significance and advanced digital infrastructure. A substantial number of cyberattacks in these areas originate from across the globe, particularly from Eastern Europe, Africa, and Asia, driven by the financial appeal of targeting major banks, multinational corporations, and high-revenue industries. Yet, these Western nations are not solely on the receiving end of cybercrime. They also play a significant role within the broader cybercrime ecosystem. Contrary to common assumptions, many malicious infrastructures, including command and control (C&C) servers, are located in Europe (Figure 51). Despite the coordinated cybersecurity efforts of European Union member states, cybercriminals frequently exploit hosting environments in countries like the Netherlands and Germany to operate compromised servers.

The United Kingdom, in particular, has seen a notable share of cybercriminal activity. One striking example occurred in 2022, when two young British individuals were arrested as part of a global investigation into the notorious Lapsus$ group. This hacking collective had executed major breaches against high-profile technology firms, including Microsoft. Their case underscores modern cybercrime's dynamic, borderless nature and the critical need for sustained international collaboration and proactive cybersecurity strategies.



Firstseen (UTC)	Host	Malware	Status	Network (ASN)	Countr
2025-01-13 14:40:25	185.77.174.191	QakBot	Offline	AS34920 SIMPLY-ROMFORD	GB
2024-03-26 23:30:12	158.220.95.215	Pikabot	Offline	AS51167 CONTABO	GB
2024-03-26 23:30:07	213.199.41.33	Pikabot	Offline	AS51167 CONTABO	DE
2024-03-05	84.46.240.42	Pikabot	Offline	AS51167 CONTABO	DE
2023-08-16 17:22:14	173.206.129.159	QakBot	Offline	AS6407 PRIMUS-AS6407	CA
2023-08-11 15:22:42	75.156.126.33	QakBot	Offline	AS852 TELUS Communications	CA
2023-08-12 11:22:45	86.222.77.167	QakBot	Offline	AS3215 France Telecom - Orange	FR
2023-08-05 18:23:16	86.222.92.165	QakBot	Offline	AS3215 France Telecom - Orange	FR

Figure 51 - Some C&C servers delivering malware are in North America and Europe.

4.5.2. Eastern European Countries



Eastern Europe remains a significant epicenter of cybercriminal activity, with Russian-speaking actors standing out for their advanced technical capabilities and well-structured operations, particularly within ransomware circles. This cybercrime ecosystem extends far beyond Russia's borders, drawing in individuals from former Soviet states such as Ukraine, Belarus, Moldova, Latvia, and Kazakhstan. While *"Russian-speaking cybercriminals"* broadly encompasses actors across this region, experts can often distinguish them through linguistic and cultural nuances. Differences in slang, forum behavior, and communication styles offer subtle yet telling geographic or national identity indicators.

The geopolitical conflict between Russia and Ukraine has introduced internal fractures within the cybercriminal underground, exemplified by infighting and ideological splits in groups like the now-defunct Conti ransomware collective. Most Russian-speaking cybercriminals, excluding state-linked Advanced Persistent Threat (APT) groups, operate in Russian-language environments, particularly underground forums such as XXS.is, Exploit.in, and Ramp, as well as encrypted platforms like Telegram (Figure 52). These digital spaces function as central hubs for collaboration, recruitment, and the trading of illicit tools and services, showcasing the resilience and the sophistication of this evolving cybercriminal ecosystem.

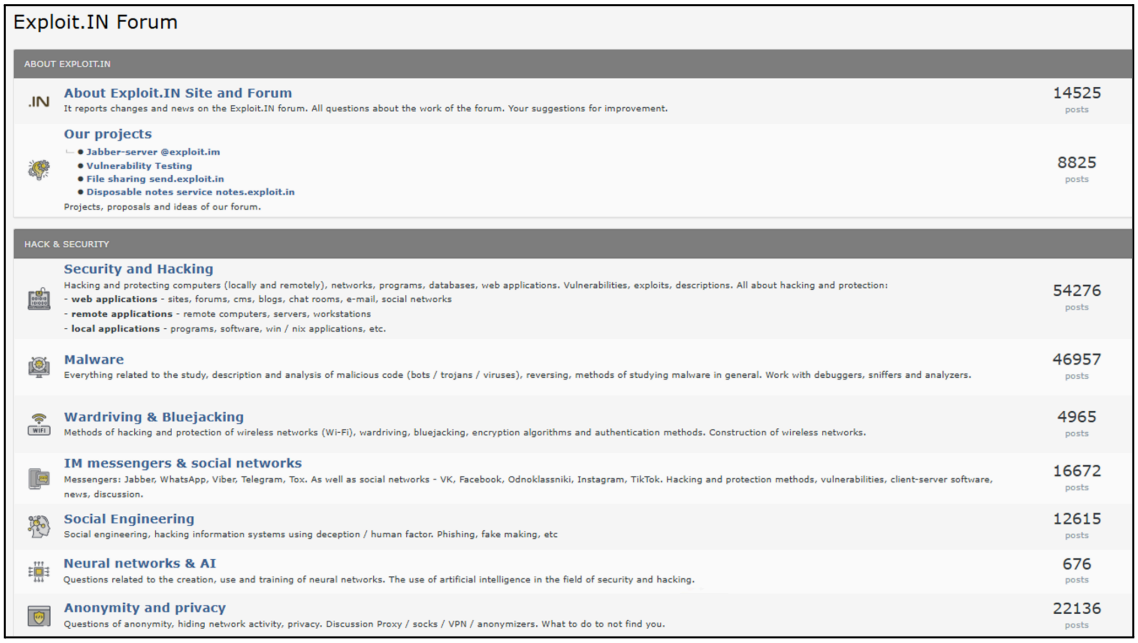


Figure 52 - Russian-speaking cybercrime forum (Source: exploit.in)

Russian-speaking cybercriminal networks are often associated with sophisticated platforms for trading stolen credentials acquired through malware such as Stealers and Remote Access Trojans (RATs). These marketplaces operate with a high degree of organization, regularly updating vast repositories containing logs from hundreds of thousands of compromised computers and servers across the globe (Figure 53). The economic hardship prevalent in many Russian-speaking regions is a significant factor fueling this prolific cybercrime ecosystem. Numerous actors active on Russian-language forums originate from former Soviet states where low income levels and limited opportunities have driven them to exploit cybercrime as a lucrative and comparatively low-risk means of income.

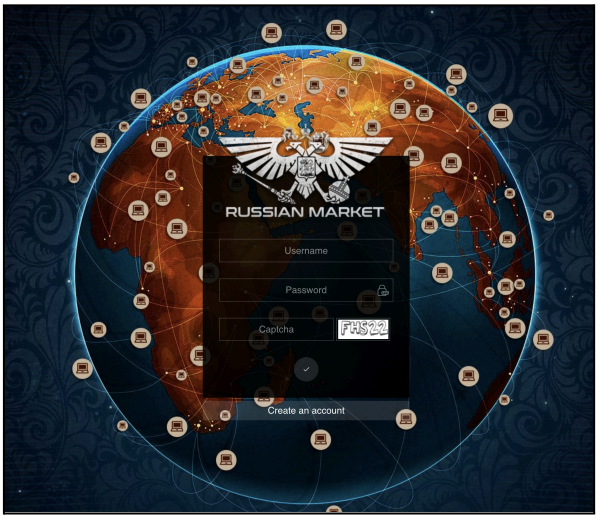


Figure 53 - A dark web logins market (Source: Russian market)

4.5.3. Middle East and African Countries



Cybercriminal activity across the Middle East and Africa exhibits marked geographic disparities, influenced by factors such as internet penetration, economic development, and the robustness of cybersecurity infrastructure. Within Africa, South Africa emerges as a principal cybercrime hub, accounting for a significant share of regional cyber threats. According to Interpol's Africa Cyber Threat Assessment 2024, South Africa is the target of 22% of all cyberattacks on the continent, with 25% of dark web communications specifically targeting organizations there, particularly government institutions. Kenya also faces considerable cyber challenges, having experienced 114 attacks on critical infrastructure in 2024 alone, and detected over 657 million cyber threats between July and September. Egypt accounts for 13% of cyberattacks across Africa, reflecting its growing exposure to digital threats.Meanwhile, Ghana recorded a dramatic surge in data breaches, with a staggering 997% increase in the first quarter of 2024 compared to the previous quarter, culminating in approximately 1.2 million breaches. Nigeria ranks prominently on the global cybercrime stage, fifth in the Global Cybercrime Index, the highest-ranking African nation. The country is frequently implicated in various cybercriminal schemes, including online scams, sextortion, romance fraud, and other illicit activities.

Although Israel is not considered a primary cybercrime hub, it is a notable source of various online scams, including fraudulent binary options, Forex and cryptocurrency schemes, call center fraud, real estate scams, investment fraud, and business email compromise (BEC) attacks. In the Maghreb region, Morocco stands out for its exposure to specific cyber threats. INTERPOL's report identifies Morocco as the African country most affected by Trojans and banking malware, with 18,827 detections. Morocco also ranks second in Africa for ransomware attacks, responsible for 8% of all incidents on the continent. The Global Cybercrime Index places Morocco seventh in Africa and 48th globally, with a score of 0.45 out of 100. In the Gulf region, countries are primarily victims rather than perpetrators. Their abundant natural resources and dynamic economies make them attractive targets for cybercriminals seeking financial gain and sensitive information.

4.5.4. South American Countries

Cybercrime across South America presents a diverse and complex picture, with distinct patterns emerging from country to country. Technical expertise, socio-economic conditions, and the robustness of legal frameworks influence these variations. In 2024, South American nations faced various cyber threats shaped by their unique environments.



- **Brazil** experienced a marked surge in cybercrime activity, particularly ransomware attacks. The Group IB annual report highlights a 19% rise in ransomware incidents compared to the previous year. The country has also become a hotspot for developing sophisticated banking malware targeting online financial transactions. Brazilian cybercriminals are notably active in credit card fraud and ATM skimming operations.

- **In Argentina**, malware targeting computers and mobile devices emerged as a primary concern, making it one of the most affected Latin American countries. Phishing campaigns have intensified, focusing on financial institutions and local businesses. Cybercriminals frequently employ social engineering tactics to extract sensitive personal and banking information.

- **Chile** faces persistent ransomware attacks and data breaches targeting businesses and government institutions. These exploits often capitalize on inadequate cybersecurity defenses within these sectors.

- **Colombian** cybercriminal groups are particularly known for their expertise in business email compromise (BEC) scams. They specialize in intercepting and redirecting payments by impersonating legitimate organizations, causing significant financial losses.

- **In Paraguay**, a rise in cryptojacking incidents and fraudulent cryptocurrency schemes has been observed, fueled by growing local interest in digital assets. These scams tend to prey on unsuspecting investors, resulting in substantial financial damage.

- **Peru** is grappling with increasing cases of e-commerce fraud and the online sale of counterfeit goods, impacting both consumers and legitimate businesses.

- **Uruguay** has seen a rise in financial fraud involving cloned payment cards used to withdraw cash illicitly from ATMs across the country. The ongoing economic instability in Venezuela has contributed to a surge in gift card fraud and cryptocurrency scams. These schemes often target victims beyond national borders, exploiting the vulnerabilities created by economic hardship.

- **Bolivia** reports widespread use of social media platforms by cybercriminals to conduct scams and identity theft, leveraging the high engagement on these networks to deceive users.

4.5.5. Asian Countries

The geographic distribution of cybercriminal activity in the Asian region varies considerably due to significant differences in terms of economic development, internet penetration, digital infrastructure, and regulatory environments. Moreover, some countries are more prepared due to a better cybersecurity culture and development.



Cybercriminal activities in **China** encompass a range of illicit activities, including hacking, online fraud, and data breaches, both within the country and beyond its borders. Industrial espionage targets intellectual property and government systems around the world. Chinese hackers generally have high technical skills and use a certain level of sophistication.

- **Japan and South Korea** are rather the major sources of cybercrime. Due to their high level of digitalization and wealth, they are often targeted by ransomware and phishing attacks. These countries have robust cybersecurity measures but face persistent threats.
- **India** is a source and target of cybercrime, with a growing number of hacking groups and financial fraud schemes. Large-scale attacks target critical infrastructure, banks, and e-commerce platforms.
- In **Pakistan,** cybercriminal operations often focus on fraud, phishing, and politically motivated attacks. Cross-border cyberattacks with India are a notable aspect.
- **Due to weaker cybersecurity frameworks and rapid digitalization, Malaysia, Indonesia, and Vietnam** are emerging hubs for cybercriminal activities. Typical activities include phishing, ransomware, and digital fraud. Indonesia has the highest rate of scams and phishing in the region.
- The **Philippines** is known for online scams and fraud targeting victims worldwide. The country hosts cybercriminal call centers and fraudulent activities related to financial scams.
- Finally, regarding **Singapore**, despite the Interpol cyber center and strong development of the cybersecurity culture, the country is seen as a victim rather than a source due to its wealth and role as a financial center.

Chapter 5: State-Sponsored Cyber Activities

State-sponsored cyber warfare has evolved into one of the most consequential forms of geopolitical competition in the modern era. Far more than a technical phenomenon, it reflects shifting power dynamics in the international system, an extension of statecraft by digital means. These operations encompass a broad spectrum of activities, including espionage, sabotage, disinformation, and cyber defense, all conducted in and through cyberspace by national governments or proxy actors acting on their behalf. The origins of state-sponsored cyber operations trace back to the Cold War, when early efforts in electronic surveillance and signals intelligence laid the groundwork for today's cyber capabilities. The digitization of warfare and intelligence accelerated in the 1990s and early 2000s, as military planners and intelligence agencies began to explore cyberspace not just as a medium for communication but as a battlespace in its own right. Landmark events such as the Chinese-led Titan Rain campaign (targeting U.S. defense networks), Russia’s cyber assaults on Estonia and Georgia, and the U.S.-Israeli deployment of Stuxnet against Iran’s nuclear infrastructure marked critical inflection points demonstrating how software could be weaponized with strategic precision and plausible deniability.

At the center of these operations are Advanced Persistent Threats (APTs) highly specialized groups often embedded within military, intelligence, or quasi-state institutions. These units operate with a level of discipline and coordination akin to special operations forces in the physical world. They utilize sophisticated tools, including zero-day vulnerabilities, spear-phishing campaigns, customized malware, and lateral movement tactics designed to quietly infiltrate and remain within targeted systems for extended periods. Their objectives range from the silent theft of state secrets and intellectual property to sabotaging critical infrastructure and influencing democratic processes. The implications of this evolution are far-reaching. Cyberwarfare has permanently altered the strategic landscape by eroding the clear boundaries between war and peace, offense and defense, domestic and international. The invisibility of cyber actors and the difficulty of attribution have empowered states to engage in continuous, low-intensity conflict beneath the threshold of open warfare. This creates an environment of persistent uncertainty, where digital skirmishes can escalate into diplomatic crises or contribute to broader geopolitical instability. In response, nations are investing heavily in both offensive and defensive cyber capabilities, forging new doctrines that treat cyberspace as a domain of warfare equal to land, sea, air, and space. Yet even as governments build resilience and response mechanisms, the inherent asymmetries of cyber conflict, where smaller nations or non-state actors can compete with superpowers, ensure that this arena will remain one of the most volatile and defining battlegrounds of the 21st century. Cyberwar operations can be classified into three broad categories:

Cyber Espionage (Intelligence Collection Operations):

Cyber espionage involves unauthorized access to confidential information held by governments, corporations, or individuals, primarily for strategic advantage. State actors deploy APTs to infiltrate networks, exfiltrate data, and monitor communications over extended periods. These operations often target intellectual property, diplomatic communications, and defense-related information. For instance, China's PLA Unit 61398 has been implicated in extensive cyber espionage activities against U.S. entities to bolster China's economic and military capabilities. Similarly, Iran's APT34 has targeted energy and telecommunications sectors in the Middle East to gather intelligence. The clandestine nature of cyber espionage makes it a preferred tool for states to gain insights without overt aggression, challenging traditional notions of sovereignty and international law.

Cyber Sabotage (Offensive Operations Disrupting and Affecting Infrastructures):

Cyber sabotage refers to deliberate actions to disrupt, degrade, or destroy critical infrastructure through digital means. These operations can have tangible, real-world consequences, such as power outages, financial disruptions, or compromised safety systems. A notable example is the 2015 cyberattack on Ukraine's power grid, attributed to Russia's Sandworm group, which caused widespread blackouts. Another instance is the Stuxnet worm, a joint U.S.-Israeli operation that targeted Iran's nuclear centrifuges, setting back its nuclear program. Cyber sabotage allows states to exert pressure or retaliate without conventional military engagement, raising concerns about escalation and protecting civilian infrastructure.

Cyber Influence (Disinformation and Manipulation Operations):

Cyber influence operations aim to shape public perception, manipulate narratives, and interfere in political processes through digital platforms. These campaigns often involve the dissemination of disinformation, propaganda, and amplifying divisive content via social media and other online channels. Russia's interference in the 2016 U.S. presidential election, involving the spread of fake news and the hacking of political entities, exemplifies the potency of such operations.

Similarly, during Operation Sindoor in 2025, India and Pakistan engaged in extensive disinformation campaigns, utilizing AI-generated content to sway public opinion and international perception. Cyber influence operations challenge democratic institutions, erode trust in information sources, and complicate diplomatic relations.

5.1 Overview of The Main Global Cyber Conflicts

5.1.1 China vs Taiwan vs United States

In 2025, the cyber conflict involving China, Taiwan, and the United States has reached unprecedented sophistication and intensity. China has amplified its state-sponsored cyber operations, particularly targeting U.S. telecommunications and infrastructure sectors, as revealed by a major breach involving eight telecom companies. These operations are spearheaded by groups such as “Volt Typhoon,” designed to extract data and maintain persistent access for future strategic disruption. China’s cyber activities are closely tied to its geopolitical ambitions, namely, unification with Taiwan and technological self-sufficiency, prompting a digital front in its confrontation with the U.S. and allies. Taiwan, increasingly caught in the middle, has become a digital battleground where Chinese cyberattacks have systematically targeted its government, military logistics, and semiconductor sectors. These operations often coincide with real-world PLA military exercises around the Taiwan Strait, highlighting a hybrid war doctrine that merges cyber and kinetic threats. In response, the United States has not only reinforced Taiwan’s cyber defense capacity through direct assistance and intelligence sharing. Still, it has also expanded sanctions and export controls on AI chips and semiconductors to curb Beijing’s technological ascent. The result is a cyber cold war where espionage, sabotage, and deterrence are conducted via invisible algorithms rather than tanks or missiles.

5.1.2 Israel vs Iran

The long-running covert war between Israel and Iran has taken on increasingly digital dimensions in 2025, characterized by precision cyber strikes on critical infrastructure and intelligence assets. Both nations have institutionalized offensive cyber capabilities into their national defense frameworks, using them to exert pressure without triggering open warfare. Iran has continued to support and develop a network of cyber militias and advanced persistent threat (APT) groups, which have targeted Israeli water systems, transit networks, and power grids, while simultaneously launching disinformation campaigns aimed at destabilizing Israel’s internal politics. In return, Israel’s cyber units, likely operating under its military intelligence, have intensified their campaign to disrupt Iran’s nuclear enrichment programs, missile command systems, and financial institutions. These attacks are surgical and highly selective, often designed to degrade capabilities without escalating into outright war. The geopolitical situation in Gaza and Lebanon has added urgency to this cyber front, with fears that digital strikes could either be preludes or reactions to physical confrontations. Notably, Iran has deepened its cyber cooperation with Russia and China, creating a more resilient offensive ecosystem that complicates Israeli defense postures. As both sides scale up their digital arsenals, cyber becomes a central pillar of their deterrence doctrines, raising the stakes of miscalculation and proxy escalation in the region.

5.1.3 India vs Pakistan

India and Pakistan's cyber rivalry has intensified significantly in 2025, mirroring their traditional border tensions and proxy conflicts. Following the deadly Pahalgam terror attack, Indian cyber agencies have reported an overwhelming surge of over 100 million cyber strikes ranging from defacements and phishing campaigns to more sophisticated malware infiltrations aimed at compromising military and government systems. Many of these attacks have been traced to Pakistan-based hacker groups with alleged state backing, such as Transparent Tribe and APT-C-23, known for conducting espionage and targeting Indian infrastructure and intelligence assets. These groups have shown a growing ability to bypass traditional security measures and conduct long-term infiltration of Indian digital systems. Conversely, India has ramped up its defensive capabilities through improved coordination between its Computer Emergency Response Team (CERT-In), private sector cybersecurity firms, and the armed forces. There are also increasing signs of retaliatory operations by Indian cyber units, though the government maintains strategic ambiguity around such actions. The digital domain has thus become an extension of the Line of Control, where covert operations unfold without the immediate risk of kinetic escalation, but with the potential to catalyze larger geopolitical consequences should a cyber incident spiral out of control.

5.1.4 Russia vs Ukraine

The cyber war between Russia and Ukraine continues to evolve as a central front in their ongoing conflict. Unlike earlier stages of the war, which were dominated by brute-force DDoS attacks and ransomware campaigns, the 2025 landscape is marked by deeply integrated hybrid operations where cyberattacks are synchronized with kinetic strikes. Ukraine has adopted an offensive cyber doctrine, recently demonstrated in "Operation Spiderweb," which combined drone assaults on Russian airbases with simultaneous digital disruptions of Russian radar and logistics systems. These multi-domain operations aim to degrade Russian coordination and delay response times. Meanwhile, Russia continues to deploy both state and proxy hacker groups to target Ukraine's civilian infrastructure, command systems, and Western allies. Groups like Killnet and NoName057(16) have escalated their activities to include symbolic DDoS attacks and more complex espionage and wiper malware targeting NATO-aligned countries.

Using a newly discovered Linux zero-day vulnerability (CVE-2024-53104) has raised alarms across the West, with speculation that it has been exploited in Russian-linked campaigns. These dynamics suggest that the Russia-Ukraine cyber conflict is not just bilateral but global in its implications, affecting everything from transatlantic policy coordination to European critical infrastructure. As both nations refine their tactics and expand their digital reach, the cyber battlefield remains one of the most volatile and high-stakes arenas of the war.

5.1.5 Other Theaters and Emerging Dynamics

Beyond the headline conflicts, cyber warfare is increasingly shaping global power dynamics in subtler but equally significant ways. In the Middle East, Iran's cyber offensives have expanded to include Gulf nations, with particular focus on Saudi Aramco and water desalination plants, an attempt to destabilize rivals economically. Israel, meanwhile, maintains back-channel cyber communication protocols with Russia to avoid accidental escalations in Syria, though these arrangements are becoming increasingly strained. In Europe, countries like Italy and Hungary have faced retaliatory cyberattacks for their pro-Ukraine stances, underscoring how digital warfare is now a tool of coercive diplomacy. The competition over emerging technologies is also intensifying the cyber race: both the U.S. and China are using cyber means to gather intelligence on quantum computing breakthroughs and AI development. Meanwhile, the European Union's AI Act, effective as of February 2025 has introduced new compliance challenges, further complicating multilateral cybersecurity efforts. These varied theaters reflect the growing ubiquity of cyber conflict, which now permeates regional rivalries, great power competition, and ideological struggles over technology governance.

5.2 Iran's Cyber Strategy: Doctrine, Capabilities, and Operations

5.2.1 Strategic Overview of Iran's Cyber Activities

While Iran has not publicly defined an official cyberwarfare doctrine, its operational behavior demonstrates a pragmatic and targeted approach, aligned with national strategic objectives. Iranian cyber operations systematically pursue three key objectives. The first is domestic regime stability, where cyber tools are leveraged to monitor, suppress, and disrupt dissident activity. Surveillance targets include activists, journalists, and perceived agents of foreign influence. The second objective is national defense and intelligence gathering. Cyber espionage tracks adversaries like the United States, Israel, and Saudi Arabia. Intelligence is gathered to anticipate threats and inform strategic decisions. The third objective centers on foreign policy and regional influence. Iran uses cyber capabilities to project power, shape regional narratives, and influence geopolitical outcomes across the Middle East and beyond.

These cyber strategies emerged from pivotal events including the 2009 Green Movement protests and the 2010 Stuxnet cyberattack, which revealed both vulnerabilities and opportunities in cyberspace for Iran. Recent developments such as the hardline presidency of Ebrahim Raisi, the stalling of JCPOA nuclear negotiations, domestic unrest spurred by the Mahsa Amini protests, and Iran's alignment with Russia continue to shape Tehran's cyber priorities.

5.2.2 Iran’s Cyber Power: Key Institutions and Structures

The development of cyber agencies in Iran has been a strategic priority over the past two decades, driven by the country's desire to bolster national security, counter external threats, and assert its influence in cyberspace. Following increased cyber vulnerabilities and notable incidents such as the Stuxnet attack, Iran invested heavily in establishing and expanding state-controlled cyber institutions.

Central to this effort are organizations like the Islamic Revolutionary Guard Corps (IRGC) Cyber Command, the Supreme Council of Cyberspace (SCC), and the Passive Defense Organization, each playing a distinct role in shaping policy, conducting cyber operations, and securing digital infrastructure. These institutions reflect Iran’s shift toward a more coordinated and sophisticated approach to cyber power and include the following:

- **The Islamic Revolutionary Guard Corps (IRGC)** is an elite military force fiercely loyal to Iran’s Supreme Leader and maintains robust and multifaceted cyber capabilities distributed among its various subdivisions. The IRGC’s cyber operations are primarily executed by specialized units within the Basij Militia and the Qods Force, both implicated in offensive and espionage cyber activities. These units orchestrate cyber intrusions aimed at foreign governments, defense industries, academic institutions, and NGOs through techniques like spear-phishing and sophisticated social engineering campaigns. Notable IRGC-linked cyber intrusion groups include:

    - **APT35 (Charming Kitten, TA453, Cobalt Mirage):** A broad cluster of cyber espionage actors conducting targeted operations against diplomatic entities, dissidents, and journalists, using tailored phishing to gather intelligence and conduct influence operations.
    - **APT42 is a subgroup of APT35, which focuses on individuals and organizations connected to policy research, human rights advocacy, and civil society. Its emphasis is** on surveilling political opposition and international human rights bodies.
    - **Nemesis Kitten:** Operating under contract through Iranian private companies like Afkar System and Najee Technologies, this group executes covert cyber operations supporting IRGC objectives, often engaging in espionage and digital sabotage.
    - **Cotton Sandstorm (formerly NEPTUNIUM):** A sophisticated IRGC-linked threat actor engaged in broad espionage campaigns targeting geopolitical adversaries and critical infrastructure.

- **Ministry of Intelligence and Security (MOIS)** serves as Iran's primary foreign intelligence and internal surveillance agency, reporting directly to the president. Unlike the IRGC, MOIS is noted for a more technically sophisticated approach and a comparatively less ideologically driven operational style. MOIS's cyber activities emphasize targeted intrusions into critical sectors such as energy, telecommunications, maritime infrastructure, and government systems. Its cyber units are linked to several advanced persistent threat (APT) groups that conduct espionage, cyber reconnaissance, and sabotage:

    - **MuddyWater:** Known for targeting Middle Eastern governments and telecommunications firms, this group conducts espionage through custom malware and credential theft.
    - **OilRig (APT34):** Focuses on the energy sector and government organizations in the Middle East, leveraging phishing campaigns and credential harvesting to extract sensitive information.
    - **Hexane:** Engages in cyber reconnaissance and espionage, often targeting telecommunications and infrastructure entities.
    - **Agrius:** A lesser-known MOIS-linked group that conducts targeted cyber espionage operations, particularly against maritime and industrial sectors.
    - **DarkBit (DEV-1084):** Specializes in sophisticated malware development and targeted intrusion campaigns primarily aimed at regional adversaries.

While MOIS and IRGC share overlapping mission scopes, MOIS's cyber operations focus more on technical exploitation and intelligence collection rather than overt influence or ideological campaigns, the competition between the two agencies occasionally drives innovation and intensity in Iran's cyber warfare efforts.

5.2.3 Contracting Ecosystem

Iran heavily relies on private contractors and academic institutions to extend its cyber reach. Emennet Pasargad operates Cotton Sandstorm for the IRGC. Ravin Academy, founded by MOIS veterans, serves as a recruitment and training hub for MOIS-affiliated operators. Legacy contractors like Mabna Institute, Rana Institute, and ITSecTeam contributed to foundational cyber campaigns but have faded from recent reporting.

5.2.4 Operational Objectives and Tactics

Iranian cyber actors prioritize intelligence collection on geopolitical adversaries and domestic threats in espionage and surveillance. Oilrig targeted Jordan's Foreign Ministry in 2022 using custom malware. Domestic surveillance groups like Domestic Kitten use mobile spyware such as FurBall to track Iranian citizens. APT35 deployed TelegramGrabber, focusing on devices within Iran using Farsi-language tools. Regarding destructive cyber operations, Iran conducts cyber sabotage, often under the guise of activism or ransomware. The Shamoon attack in 2012 was a landmark, destructive incident targeting Saudi Aramco. In 2022, the Albanian cyberattack was conducted by Oilrig and Hexane under the false front HomeLand Justice. In 2023, DarkBit carried out a destructive attack on Israel's Technion Institute, masquerading as ransomware, with access handed over by MuddyWater. Iran's increasing use of deceptive hacktivist fronts suggests a strategy to obscure state involvement while enabling plausible deniability. Tehran integrates cyber operations with influence campaigns to sway public opinion and sow discord, forming the backbone of its information operations (InfoOps). Cotton Sandstorm led coordinated campaigns against targets like Charlie Hebdo and regional opponents like Bahrain. Operations often leverage fake social media accounts and fabricated personas to amplify narratives aligned with Iranian state interests. Although not Iran's primary cyber objective, financially motivated operations are sometimes conducted by IRGC-linked contractors. Fox Kitten and Nemesis Kitten have exploited vulnerabilities like Log4j for ransomware and crypto-mining campaigns. Whether these operations are sanctioned or self-directed remains unclear.

5.2.5 Target Profile and Geographical Focus

Primary target sectors include energy, a historical target notably via APT33 and Shamoon. The IRGC continues to target energy firms in the US and Gulf. Telecommunications are targeted for signals intelligence, with recent MOIS-driven campaigns by MuddyWater and Hexane focusing on Middle Eastern telecom operators. Transportation is a strategic focus given Iran's location on the Strait of Hormuz, with groups like APT35 and UNC3890 targeting shipping firms in Israel and Egypt. Critical infrastructure, though underreported in open sources, shows evidence suggesting Iran seeks to compromise US and Israeli infrastructure.
Academic, NGO, and think tank personnel are particularly targeted by APT42, focusing on Middle East policy experts, human rights activists, and political analysts. Regarding regional targeting trends, the Middle East remains Iran's main arena for cyber operations, especially against Israel and Gulf states. The United States saw increased targeting in 2022–2023, with IRGC actors showing greater boldness and sophistication. Europe and the Balkans experienced less frequent but impactful attacks, such as the Albanian government incident.

5.2.6 Evolution and Trends in Iran's Cyber Capabilities

Iranian cyber units have undergone a marked transformation in recent years, exhibiting increased technical sophistication, operational agility, and strategic coordination. Notably, their growing proficiency in exploiting zero-day vulnerabilities signals a shift toward more advanced offensive capabilities, placing them among the more formidable state-backed cyber actors. Their ability to rapidly adapt to public exposure, evident when Oilrig operations seemingly transitioned to Hexane following the 2020 leaks by Lab Dookhtegan, reflects an organizational resilience and decentralization that complicates attribution and response. A trend toward tighter intra-agency collaboration is also emerging, as seen in the coordinated activity among MOIS-affiliated groups during the Albanian cyberattacks. The involvement of Plaid Rain, a Lebanon-based actor likely connected ideologically and operationally with Hezbollah, underscores Tehran's growing reliance on regional proxies to project cyber power while maintaining plausible deniability. Looking forward, Iran is expected to refine this model of hybrid cyber warfare, integrating domestic units with proxy actors across ideological and geopolitical lines. This will likely result in more complex, multi-vector campaigns that blur the lines between state and non-state activity. Additionally, their strategic focus may include disruptive influence operations targeting elections, infrastructure, and regional rivals, especially as tensions in the Middle East and global polarization deepens. Defenders should anticipate a surge in coordinated campaigns that combine cyberespionage, data leaks, and psychological operations as these units evolve.

5.3 China's Cyber Strategy: Doctrine, Capabilities, and Operations

5.3.1 Strategic Overview of Iran's Cyber Activities

China's cyber strategy represents a comprehensive and multifaceted approach that integrates political, military, economic, and technological dimensions. At its core, this strategy is guided by the concept of "informatization," the use of advanced information and communication technologies to enhance national power and governance. The Chinese government perceives cyberspace not merely as a domain of communication or commerce, but as a crucial arena for national security, international competition, and strategic influence.

Beijing's cyber activities are orchestrated through a civil-military fusion framework, which enables seamless coordination between state agencies, private tech companies, academic institutions, and the People's Liberation Army (PLA). This synergy allows China to rapidly develop and deploy cyber capabilities that serve both defensive and offensive objectives. On the one hand, these capabilities are intended to safeguard critical infrastructure and protect state interests from foreign threats. On the other hand, they are used to conduct cyber espionage, influence operations, and potentially disable adversary systems during conflict.

5.3.2 China's Cyber Power: Key Institutions and Structure

China’s national cyber framework has profoundly evolved over the past two decades, transitioning from fragmented institutional efforts to a highly integrated system combining military strength, civilian intelligence, and centralized policymaking. This development reflects Beijing’s recognition of cyberspace as a critical domain for national security, economic resilience, and geopolitical competition. From early defensive measures to today’s sophisticated offensive and intelligence capabilities, China has constructed a layered cyber apparatus involving multiple specialized agencies. These include newly established military units like the People’s Liberation Army Cyberspace Force, long-standing civilian actors such as the Ministry of State Security, and central coordinating bodies like the Central Cyberspace Affairs Commission. Each plays a distinct but interconnected role within a strategic architecture designed to assert cyber sovereignty, shape global norms, and project digital power. The following sections will examine each of these entities in detail, tracing their origins, functions, and the ways they contribute to China's comprehensive cyber strategy.

People’s Liberation Army (PLA) Cyberspace Force

Established in April 2024, the PLA Cyberspace Force is the primary military body responsible for China’s cyber warfare. Operating under the Central Military Commission, it replaced the former Network Systems Department of the PLA Strategic Support Force. Its responsibilities include offensive cyber operations, network defense, cyber reconnaissance, and integrating electronic warfare into the broader PLA strategy.

- **Offensive Operations Division**. This unit is tasked with launching cyberattacks against foreign military networks and critical infrastructure. It is central to China's ability to disrupt adversarial command systems, gather battlefield intelligence, and execute strategic deterrence in cyberspace.

- **The Cyber Defense Division** is responsible for securing PLA information infrastructure. This unit focuses on hardening military networks against intrusions, malware, and data exfiltration attempts. It also develops defensive tools and conducts threat hunting within PLA systems.

- **Cyber Intelligence Division** conducts reconnaissance operations, including cyber surveillance and digital espionage. It collects information on adversary capabilities and supports PLA strategic planning with real-time threat data.

- **The Electronic Warfare Division** integrates cyber capabilities with electronic warfare; this unit targets satellite communications, radar systems, and battlefield sensors to disrupt enemy’s communication systems.

- **Associated APT Groups**

    - **APT3 (Gothic Panda):** Suspected to be linked to PLA contractors, this group targets aerospace and defense industries with sophisticated intrusion methods.

    - **APT40 (Kryptonite Panda):** Believed to support PLA Navy intelligence, it focuses on maritime targets, research institutions, and foreign ministries globally.

Ministry of State Security (MSS)

The MSS serves as China's civilian intelligence service and oversees the nation's covert cyber-espionage and counterintelligence campaigns. Its cyber operations are primarily conducted through the 13th Bureau and regional cyber units. The MSS maintains deep ties with contractors, universities, and front companies to expand its technical capabilities.

- **13th Bureau (CNITSEC)** is the China Information Technology Security Evaluation Center, which acts as the cyber headquarters within the MSS. Officially responsible for national cybersecurity evaluation, it covertly runs cyber-espionage campaigns, manages malware development, and exploits software vulnerabilities for intelligence collection.

- **Provincial MSS Cyber Units are** distributed across China's provinces, conducting tailored Advanced Persistent Threat (APT) operations. They often focus on regional or sector-specific targets and collaborate with local tech talent or companies under MSS direction.

- **The Chinese National Vulnerability Database (CNNVD)** is administered by CNITSEC., CNNVD is China's equivalent to a national CVE system. However, it has been caught delaying disclosure of vulnerabilities to allow MSS teams time to exploit them in the wild, turning a supposed defense database into an offensive tool.

- **Associated APT Groups**

    - **APT1 (Comment Crew):** One of the earliest known Chinese cyber units, APT1 is linked to the massive theft of U.S. intellectual property.
    - **APT10 (Stone Panda):** Known for compromising managed service providers globally to access client networks en masse.
    - **APT27 (Emissary Panda):** Specializes in targeting aerospace and defense organizations, often with backdoors and custom malware.

    - **APT31 (Zirconium / Judgment Panda):** Utilizes advanced techniques to conduct political espionage and influence operations, often impersonating Western security tools to obscure attribution.

Central Cyberspace Affairs Commission (CCAC) & Cyberspace Administration of China (CAC)

The CCAC and CAC form the strategic leadership and enforcement tier of China's cyber governance model. While the CCAC sets national-level policy in cyberspace, the CAC implements those directives through domestic regulation, censorship, and cybersecurity mandates. Together, they form the administrative foundation of China's concept of "cyber sovereignty."

- **The Central Cyberspace Affairs Commission (CCAC),** chaired by senior CCP leadership, is the highest body for internet and cyber policy in China. It coordinates civil-military integration in cyberspace and ensures that all cyber operations align with Party ideology, national security priorities, and long-term development goals.

- **Cyberspace Administration of China (CAC)** is the executive arm of the CCAC., The CAC enforces laws on data security, online content, and critical infrastructure protection. It oversees internet companies, monitors compliance, and plays a central role in online censorship, often mandating real-time cooperation from major platforms.

- **The National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC)** is China's national incident response center. It monitors malware outbreaks, coordinates cyber attack responses, and fosters partnerships with telecoms and tech firms. CNCERT also plays a significant role in framing China's international narrative around cybersecurity.

- **Associated APT Activities** While CAC and CNCERT are not directly linked to named APT groups, they indirectly enable state-sponsored cyber operations by building regulatory frameworks and infrastructure that support surveillance, content control, and domestic cyber enforcement. Their influence overlaps with APT-style capabilities used for internal repression, such as targeting dissidents and journalists.

5.3.3 Contracting Ecosystem

China employs a "military-civil fusion" strategy that integrates civilian entities into its cyber operations. State-owned enterprises (SOEs) and private firms such as Huawei, Hikvision, and SenseTime contribute to China's cyber capabilities by providing technological expertise and infrastructure. These companies often collaborate with military and intelligence agencies, effectively blurring the lines between civilian and military domains. Academic institutions, including universities and research institutes, conduct cyber research and develop tools supporting national cybersecurity objectives while serving as talent pools for recruiting cyber professionals into state-sponsored operations. Additionally, China cultivates a network of non-state actors, including patriotic hackers and cyber militias, who conduct cyber operations aligned with national interests. These groups often operate under the guidance or tacit approval of state agencies.

5.3.4 Operational Objectives and Tactics

China’s cyber operations are driven by strategic goals reflecting its broader ambitions in global power dynamics and digital sovereignty. These goals include securing national sovereignty in the digital domain, achieving technological self-reliance and supremacy, expanding global influence through digital channels, and shaping international norms and cyberspace governance in alignment with authoritarian values. China employs a multifaceted approach encompassing espionage, disruption, influence, and cybercrime to realize these objectives. Espionage remains a central pillar, with operations targeting foreign governments, military organizations, and corporations to extract political, economic, and technological intelligence, evidenced by high-profile intrusions into Dutch military networks and the Czech foreign ministry. Simultaneously, China invests heavily in cyber capabilities to sabotage critical infrastructure, such as power grids and communications systems, to prepare for potential conflict scenarios. Influence operations are also integral, leveraging AI-generated content, social media manipulation, and disinformation campaigns to sway public opinion and political landscapes abroad.

Furthermore, Chinese state-sponsored actors engage in cybercrime for financial gain, particularly through intellectual property theft and digital fraud. These operations are executed using sophisticated tactics, including spear-phishing, supply chain attacks, zero-day vulnerabilities exploitation, and tailored malware deployment. Collectively, these efforts illustrate how China views cyberspace as a strategic domain essential to national power, global influence, and long-term geopolitical competition.

5.3.5 Target Profile and Geographical Focus

China's cyber operations have a global reach but exhibit specific geographical focuses. The Asia-Pacific region is a primary focus, particularly neighboring countries involved in territorial disputes or hosting U.S. military forces. Operations in this region have included data theft from ASEAN nations and surveillance of regional military activities. Western democracies, including the United States, European Union member states, and allied countries, are targeted for political, economic, and technological intelligence, as demonstrated by recent cyberattacks on Dutch industries and the Czech foreign ministry. Nations participating in China’s Belt and Road Initiative (BRI) are also subject to monitoring, with cyber operations often focusing on infrastructure projects and political developments to ensure alignment with Chinese strategic interests.

5.3.6 Evolution and Trends in China’s Cyber Capabilities

China's cyber capabilities have undergone significant evolution. The country maintains numerous Advanced Persistent Threat (APT) groups, such as APT40 and PLA Unit 61398, which are known for conducting long-term cyber espionage campaigns with sophisticated tactics and persistent targeting of strategic sectors. Chinese cyber actors increasingly integrate artificial intelligence and machine learning into operations, using these technologies for vulnerability discovery, automated exploitation, and information operations, including generating convincing phishing content and deepfake media. A growing focus on supply chain security is also evident, with efforts to exploit vulnerabilities in global supply chains and secure Chinese technologies from foreign interference, including embedding surveillance capabilities in exported technologies. Finally, China invests heavily in cybersecurity talent development through education, training programs, and the integration of cyber curricula in academic institutions, ensuring a steady pipeline of skilled professionals for both offensive and defensive operations.

5.4 Russia’s Cyber Strategy: Doctrine, Capabilities, and Operations

5.4.1 Strategic Overview of Russia’s Cyber Activities

Russia's cyber strategy, firmly anchored in the concept of "information confrontation" (informatsionnoye protivoborstvo), reflects a holistic and persistent approach to modern warfare, blending cyber operations, psychological manipulation, disinformation, and electronic warfare into a cohesive national security tool. This doctrine emphasizes shaping perceptions and behavior on both domestic and global fronts and institutionalized cyber capabilities within the military framework, as highlighted by the establishment of specialized information operations units following the 2015 military doctrine.

These units operate offensively and defensively, leveraging a model of persistent engagement that ensures ongoing infiltration and influence within adversary networks to collect intelligence, cause disruption, and sustain strategic pressure. The seamless integration of these tactics has been particularly prominent in the conflict with Ukraine, where Russia's cyber activities serve as force multipliers for conventional military efforts, demonstrating the centrality of information warfare in its broader geopolitical agenda.

5.4.2 Russia's Cyber Power: Key Institutions and Structures

Over the years, Russia has progressively integrated cyber capabilities into its national security framework, recognizing cyberspace as a critical domain for both defense and strategic influence. This integration has involved developing and coordinating specialized institutions and agencies tasked with cyber operations, intelligence gathering, and information warfare. By embedding cyber tools within its broader security apparatus, Russia has enhanced its ability to conduct sophisticated cyberattacks, protect critical infrastructure, and project power in the digital realm. This strategic emphasis reflects a comprehensive approach where cyber activities are tightly interwoven with military, intelligence, and law enforcement functions, making cyber power a central pillar of Russia's national security posture. The following agencies represent the prominent cyber actors in Russia:

- **Main Directorate of the General Staff of the Armed Forces of the Russian Federation GRU)** is Russia's military intelligence agency and the primary actor behind the country's state-sponsored offensive cyber operations. Operating under the Ministry of Defense, it runs multiple cyber units engaged in espionage, sabotage, and information warfare.
    - **Unit 26165 (APT28/Fancy Bear)**: Specializes in cyber espionage, targeting political organizations, defense ministries, media outlets, and election infrastructure worldwide. This unit is widely believed to have interfered in the 2016 U.S. presidential election and other political events in Europe.
    - **Unit 74455 (Sandworm Team)**: Conducts large-scale destructive cyber operations. It was behind the NotPetya malware attack in 2017, which caused billions in damages globally, and cyberattacks on Ukraine's power grid. It focuses on cyber warfare capabilities to disrupt critical infrastructure.
    - **Unit 29155**: Known for physical covert operations including assassinations and sabotage abroad, such as the 2018 Skripal poisoning in the UK. It is also expanding its remit into hybrid operations that blend traditional clandestine activity with cyber tools.

- **Federal Security Service (FSB)** is Russia's principal security agency and successor to the KGB, with wide-ranging responsibilities including counterintelligence, counterterrorism, and surveillance. In the cyber domain, the FSB plays a central role in overseeing and conducting both domestic cyber defense and offensive cyber operations. It operates units specialized in hacking, cyberespionage, and information warfare, often targeting foreign governments, critical infrastructure, and private-sector organizations. The FSB is also responsible for domestic internet surveillance and censorship under programs like SORM (System of Operative Search Measures), and it enforces compliance with Russia's data localization laws. Internationally, it has been implicated in numerous cyberattacks, including election interference campaigns and operations to disrupt or steal sensitive information from Western institutions.

- **The Russian Foreign Intelligence Service (SVR)** maintains a sophisticated and competent cyber operations division, integral to Russia's broader intelligence and geopolitical strategies. The SVR's cyber capabilities include cyber espionage, advanced persistent threats (APTs), influence operations, and information warfare. Structurally, the SVR operates under a highly secretive and compartmentalized framework, with specialized units dedicated to offensive cyber operations to penetrate foreign government networks, critical infrastructure, and private sector targets worldwide. These operations are often characterized by custom-developed malware, spear-phishing campaigns, and zero-day exploits to achieve stealthy, long-term access. The SVR's cyber units frequently collaborate with other Russian intelligence and military agencies, such as the GRU (Main Intelligence Directorate), sharing intelligence and operational tactics to maximize impact. Their cyber activities are typically aligned with Russia's strategic interests, including undermining Western political institutions, stealing sensitive technological and military data, and conducting psychological operations to sow discord. The SVR's ability to integrate cyber tools with traditional intelligence collection makes it a formidable player in the global cyber espionage landscape, consistently adapting its methods in response to evolving cybersecurity defenses. The SVR includes the following cyber units:

    - **Unit 26165 (or 26166) / APT29 / Cozy Bear is** one of the most well-known SVR-linked cyber espionage groups. It is believed to focus on long-term cyber intelligence gathering. This group is known for sophisticated, stealthy intrusion campaigns against Western governments, think tanks, and diplomatic entities, often using spear phishing, malware implants, and zero-day exploits.

    - **Unit 74455 is** reported to be involved in cyber operations. It signals intelligence (SIGINT). This unit conducts offensive cyber attacks and

intelligence gathering, possibly specializing in the technical exploitation of foreign networks.

    - **Information Operations and Influence Units** are not purely cyber. Still, these units work closely with cyber teams to conduct coordinated information warfare, leveraging cyber access to steal and leak sensitive data, amplify disinformation campaigns, and manipulate public opinion.
    - **Support and Infrastructure Units** manage the cyber infrastructure that supports operations, such as command-and-control servers, encrypted communications, and secure data exfiltration channels, ensuring operational security and persistence.

- **Federal Service for Technical and Export Control (FSTEC)** is Russia's primary agency for protecting state secrets and critical information infrastructure. It plays a regulatory and enforcement role in cybersecurity policy, focusing on information assurance, secure software certification, and the protection of classified data from foreign technical intelligence. FSTEC issues security requirements for IT products and networks used in government and military settings and mandates compliance through audits and inspections. It also controls the export of cryptographic technologies and dual-use software. While less directly involved in offensive cyber operations, FSTEC contributes to national cyber defense by setting technical standards and working closely with the FSB and other entities to secure state-run information systems.
- **Institute of Cryptography, Telecommunications and Computer Science (IKSI)** is an academic and research institution affiliated with the FSB, tasked with developing advanced capabilities in cryptography, secure communications, and cyber defense technologies. It serves as a training ground for cyber operatives and engineers who go on to work in Russia’s intelligence and defense sectors. IKSI conducts cutting-edge research in mathematical algorithms, encryption systems, secure coding, and countermeasures against foreign cyber threats. Its role is strategic and scientific, providing the intellectual and technological foundation for Russia's cyber capabilities.

  The institute supports both defensive and offensive missions by developing tools and expertise used by agencies like the FSB and the Ministry of Defense

5.4.3 Contracting Ecosystem

Russia employs a complex ecosystem comprising state-sponsored actors, private companies, and non-state proxies to conduct its cyber operations. State-sponsored Advanced Persistent Threats (APTs) are highly advanced and closely integrated with Russia's intelligence services, executing espionage, information theft, and disruption missions. Organized Crime Groups (OCGs), primarily financially motivated, dominate the ransomware landscape and often operate with tacit approval from the state. They commonly use Ransomware-as-a-Service (RaaS) models, where ransomware developers lease tools to affiliates who carry out attacks. Private cybersecurity firms, including Positive Technologies, have been implicated in supporting state cyber activities by providing specialized tools and expertise. Hacktivist groups like CyberBerkut conduct DDoS attacks and information campaigns as pro-Russian actors, frequently suspected of having links to Russian intelligence agencies.

5.4.4 Operational Objectives and Tactics

Russia’s cyber operations serve multiple strategic objectives, each aligned with broader national interests. Foremost among these is intelligence collection, with cyber espionage targeting governmental agencies, military institutions, and key industrial sectors to acquire sensitive data and strategic insight. Equally prominent is the objective of disruption, exemplified by sophisticated attacks on critical infrastructure such as the 2015 and 2016 intrusions into Ukraine’s power grid designed to undermine state stability and project coercive power. Influence operations represent another pillar, leveraging coordinated disinformation campaigns to polarize societies, erode trust in democratic institutions, and sway electoral outcomes, particularly in Western democracies. Economic motivations also drive Russian cyber activities, with state-linked or state-tolerated actors conducting ransomware attacks and other financially motivated cybercrimes. Operationally, Russia employs advanced techniques including spear-phishing, supply chain attacks, exploitation of zero-day vulnerabilities, and deployment of tailored malware. These efforts are often synchronized with conventional military and political strategies, reflecting an integrated approach to hybrid warfare that blurs the boundaries between war and peace, state and non-state actors, and physical and digital domains.

5.4.5 Target Profile and Geographical Focus

Russia’s cyber operations are global in scope but prioritize specific targets. Ukraine remains a central focus, with attacks to disrupt military capabilities and critical infrastructure. Western nations, particularly those supporting Ukraine,such as the United States and EU member states, are targeted for intelligence collection and disruption of aid logistics. International organizations like NATO and the Organization for the Prohibition of Chemical Weapons (OPCW) have also been subjected to cyber espionage efforts.

Additionally, the private sector is frequently targeted for intelligence and disruptive purposes, especially in the defense, energy, and technology industries.

5.3.6 Evolution and Trends in Russia's Cyber Capabilities

Russia's cyber capabilities have evolved significantly in recent years. The country has shifted from using commodity malware to developing sophisticated, custom malware with advanced cryptographic and anti-analysis features. Russian cyber actors are increasingly integrating emerging technologies such as artificial intelligence and machine learning to enhance the effectiveness and stealth of their operations. A persistent engagement strategy is evident, focusing on maintaining long-term access to target networks for continuous intelligence gathering and operational readiness. Moreover, the blending of cyber operations with conventional military tactics obvious in the Ukraine conflict, illustrates Russia's commitment to hybrid warfare as a core component of its cyber doctrine

5.5 North Korea's Cyber Strategy: Doctrine, Capabilities, and Operations

5.5.1 Strategic Overview of North Korea's Cyber Activities

North Korea's cyber strategy has emerged as a core component of its asymmetric warfare doctrine, designed to offset its conventional military inferiority and economic isolation. Under the leadership of Kim Jong-un, Pyongyang has aggressively expanded its cyber capabilities, transforming them into a strategic tool for national security, regime survival, and economic sustenance. The strategic doctrine guiding these activities is rooted in the state's broader objective of countering perceived external threats, particularly from South Korea, the United States, and their allies, while exploiting cyber operations for financial gain and intelligence gathering. Unlike traditional cyber powers prioritizing defense and deterrence, North Korea's cyber doctrine is offensive, covert, and opportunistic. It emphasizes deniability and indirect confrontation, exploiting the blurred lines of attribution in cyberspace. Cyber operations offer North Korea a unique combination of stealth, impact, and low cost, allowing it to strike adversaries without risking direct military retaliation. These operations serve strategic functions such as destabilizing hostile nations, demonstrating technical sophistication, and acquiring hard currency through illicit cyber means.

North Korea's actions in cyberspace form part of a broader pattern of gray-zone conflict, where cyberattacks are used to manipulate the strategic environment below the threshold of armed conflict.

5.5.2 North Korea's Cyber Power: Key Institutions and Structures

North Korea's cyber operations are governed by a highly centralized and hierarchical structure, reflecting the tight control of the ruling regime. At the heart of this institutional architecture is the following

- **The Reconnaissance General Bureau (RGB)**, serves as the primary agency responsible for overseeing the country's cyber activities. As the main military intelligence arm of the Korean People's Army, the RGB is the central command hub for offensive cyber operations. It reports directly to the State Affairs Commission, chaired by Kim Jong-un, indicating the strategic importance placed on cyber warfare at the highest level of North Korea's leadership. Within the RGB, Unit 121 is widely believed to be the most prominent division tasked with executing offensive cyber missions. It plays a leading role in North Korea's cyber warfare efforts and is often implicated in cyberattacks targeting foreign governments, critical infrastructure, and private entities. The unit comprises highly skilled operatives trained to conduct various cyber sabotage and espionage forms. Several subordinate groups operate under or in close coordination with the RGB. Among the most well-known is the Lazarus Group, which has gained international notoriety for its involvement in cyber-espionage and destructive attacks, including the 2014 Sony Pictures hack. The group has been linked to various cyber activities to advance the regime's political and military objectives.

    - **APT38**, which focuses primarily on financial cybercrime. This group is responsible for numerous high-profile bank heists and cyber-enabled thefts aimed at generating hard currency for the North Korean regime. APT38 is known for its sophisticated tactics, including long-term intrusions into banking systems and SWIFT networks.

    - **Andariel** is another cyber unit affiliated with North Korea's offensive operations. It focuses on cyber-espionage and attacks specifically targeting South Korea's government and defense sectors. It is believed to operate with a degree of autonomy while remaining within the broader command structure of the RGB.

    - **The Technical Reconnaissance Bureau (TRB)** plays a supporting role by providing signals intelligence (SIGINT). The TRB operates as part of the broader military intelligence apparatus, contributing electronic surveillance and intelligence-gathering capabilities that complement offensive cyber missions.

- **The Ministry of State Security (MSS)** also contributes to the cyber apparatus by handling internal counterintelligence. Its role primarily focuses on ensuring loyalty within cyber units, preventing defection or unauthorized activity, and securing the internal communications and operations of North Korea's cyber personnel.

These cyber units are composed of elite operatives recruited from the country's most prestigious institutions, such as Kim Il-sung University and the University of Automation. Selected individuals undergo rigorous training both domestically and abroad, particularly in countries like China and Russia, to acquire advanced technical skills and exposure to global cyber tactics.

5.5.3 Contracting Ecosystem

North Korea's cyber strategy increasingly relies on a dispersed and globally embedded contracting ecosystem to mask attribution, access foreign infrastructure, and evade international sanctions. This ecosystem includes front companies, proxy developers, and overseas IT contractors stationed in China, Southeast Asia, and parts of Africa and Eastern Europe. These operatives are often embedded in legitimate tech firms or freelance marketplaces under false identities, providing software services to unwitting clients while siphoning off data or generating revenue for the regime.

This cyber-labor force not only functions as a funding mechanism but also as a reconnaissance tool. Contractors collect valuable information about clients' infrastructure, which can later be exploited in targeted cyber operations. These workers remit their earnings to the North Korean state, often under the supervision of RGB liaisons, highlighting the convergence of cyber strategy and economic strategy in North Korea's broader statecraft. Using this contracting ecosystem blurs the distinction between state and non-state actors, creating legal and diplomatic challenges for attribution and retaliation.

5.5.4 Operational Objectives and Tactics

North Korea's cyberstrategic objectives are varied, ranging from political and military to economic. Politically, these operations often aim to intimidate adversaries, undermine public trust in institutions, and retaliate for perceived insults to the regime, as demonstrated by the 2014 Sony Pictures hack.

Militarily, cyber tools are used to gather intelligence on enemy capabilities and defense systems, thus providing a strategic advantage without physical confrontation. Economically, cybercrime has become a significant source of revenue for the regime, especially in the face of stringent international sanctions. Tactically, North Korean operators employ a broad spectrum of cyber tools, including spear phishing, ransomware, wiper malware, and supply chain attacks. Their operations often begin with social engineering to gain initial access, followed by lateral movement within networks to escalate privileges and exfiltrate data or deploy destructive payloads. Sophisticated techniques such as domain fronting, encrypted command and control infrastructure, and living-off-the-land binaries reflect a growing technical maturity. North Korean hackers are also adept at obfuscating their digital

footprints, frequently routing traffic through global infrastructure and reusing tools with minor modifications to complicate detection.

5.5.5 Target Profile and Geographical Focus

The target profile of North Korea's cyber operations is diverse and global, reflecting its multifaceted strategic interests. Financial institutions and cryptocurrency exchanges have been particularly prominent targets, serving both as revenue sources and as soft targets with relatively weak cyber defenses. The 2016 Bangladesh Bank heist and a string of cryptocurrency thefts in subsequent years underscore the regime's focus on financial cybercrime. Beyond economic targets, North Korea has routinely targeted defense contractors, government agencies, media organizations, and academic institutions, especially those in South Korea, the United States, and Japan. These operations aim to extract intelligence, disrupt military readiness, and erode trust in democratic institutions. Geographically, while the Korean Peninsula remains the epicenter of strategic interest, North Korea's cyber reach extends to Southeast Asia, Europe, the Middle East, and even Africa, exploiting global vulnerabilities and financial systems. Moreover, North Korea's targeting strategy is dynamic and opportunistic. It adapts rapidly to geopolitical developments, such as shifts in sanctions regimes, diplomatic tensions, or technological trends, by recalibrating its targets and objectives. This flexibility enables Pyongyang to continuously exploit openings in a fast-changing global digital landscape.

5.5.6 Evolution and Trends in North Korea's Cyber Capabilities

North Korea's cyber capabilities have significantly evolved over the past two decades, from rudimentary website defacements to highly sophisticated, multi-stage attacks capable of global disruption. Early operations in the 2000s relied on basic denial-of-service attacks and low-grade espionage. However, by the mid-2010s, groups like Lazarus had begun executing complex financial intrusions and ransomware campaigns, such as WannaCry in 2017, which infected over 200,000 systems across 150 countries.

In recent years, the technical sophistication of North Korean operations has grown markedly. Operators now employ advanced evasion techniques, custom malware strains, and modular toolkits often indistinguishable from those used by top-tier nation-state actors. Their operations increasingly integrate techniques borrowed from the private cybersecurity world, such as open-source exploitation frameworks and commodity malware kits, demonstrating adaptive learning and reverse engineering capabilities. Additionally, North Korea has shown interest in exploiting emerging technologies, such as artificial intelligence for enhanced phishing or malware distribution. It has explored vulnerabilities in blockchain protocols to target decentralized finance systems. The regime's continuous investment in training cyber

personnel and integrating cyber into broader intelligence and military structures suggests that its offensive cyber capabilities will continue to evolve, posing an enduring and asymmetric threat to global digital and economic systems.

5.6 Israel's Cyber Strategy: Doctrine, Capabilities, and Operations

5.6.1 Strategic Overview of Israel's Cyber Activities

Israel's cyber strategy is deeply rooted in its national security doctrine, prioritizing preemption, intelligence superiority, and strategic deterrence. Given the persistent threats from regional adversaries such as Iran, Hezbollah, and Hamas, as well as broader global cyber threats, Israel has developed a proactive and integrated cyber posture. The nation treats cyberspace as a key domain of warfare, on par with air, land, sea, and space. The 2017 launch of Israel's National Cyber Directorate (INCD) unified civil and military cyber efforts, establishing a doctrine that blends offensive capabilities with robust national defense. Strategic cyber activities range from infrastructure protection and cyber threat intelligence (CTI) sharing to coordinated offensive campaigns designed to degrade adversary command and control systems or disrupt critical infrastructure. This strategy is also tied to broader geopolitical objectives, including counterterrorism, surveillance, and the containment of regional actors via clandestine and hybrid warfare methods.

5.6.2 Israel's Cyber Power: Key Institutions and Structures

Israel has established itself as a global leader in cybersecurity by integrating cyberspace across its national infrastructure, both military and civilian. The country operates a complex ecosystem of cyber entities, including the following:

- **Israel Military Intelligence (Aman)** , the intelligence branch of the Israel Defense Forces, is responsible for strategic intelligence collection, analysis, and operations, and it commands some of the most elite cyber units in the world. Aman's two most notable cyber entities are Unit 8200 and Unit 81. Unit 8200 specializes in signals intelligence (SIGINT), cyber espionage, and offensive cyber operations.

  It is the largest and most technologically advanced unit in the Israeli military and serves as the backbone of cyber-intelligence gathering against hostile states and organizations. Unit 81, operating closely with 8200, develops advanced technologies, including offensive cyber tools, specialized hardware, and encryption-breaking systems, to support operations by the intelligence and special forces community. It is important to note that these units are not under the command of the IDF's C4I & Cyber Defense Directorate, but rather under the authority of its Military Intelligence (Aman). They are critical components of Israel's strategic cyber warfare capability, particularly for external operations and intelligence dominance.

- **The Israel Defense Forces C4I and Cyber Defense Directorate** are separate from Aman. The C4I and Cyber Defense Directorate (the J6 & Cyber Defense Directorate) is a branch of the IDF General Staff focused on cyber defense, military IT systems, and secure communication. This directorate oversees several specialized units responsible for infrastructure and defensive cyber operations. Mamram is the IDF's central computing unit, in charge of developing and managing software systems, databases, and military IT infrastructure. Matzov (Center for Encryption and Information Security) develops encryption technologies and secures IDF and national communication systems. Hoshen focuses on civilian communications networks, while Maof serves as a command-and-control center for cyber defense operations, including real-time threat detection and response across IDF systems. Unlike Aman's units, which are outward-facing and intelligence-driven, the C4I Directorate's mission is internal: to protect IDF networks and enable secure operational functionality.

- **The Mossad's cyber units,** operating under Israel's foreign intelligence service, play a critical role in covert operations aimed at advancing national security objectives beyond Israel's borders. While less publicly recognized than the military's Unit 8200, these clandestine teams specialize in offensive cyber actions that align with Mossad's broader intelligence missions. Their operations often target hostile regimes, disrupt Iran's nuclear ambitions, or pave the way for physical missions through digital sabotage.
  Using tools such as malware, system breaches, and psychological cyber tactics, Mossad's cyber operatives execute stealthy intrusions and data theft, prioritizing deniability and synchronization with field operations to maintain their covert edge.

- **Shabak (Israel Security Agency) Cyber Defense and Counterterrorism** Shabak, also known as Shin Bet, is responsible for domestic security, counterterrorism, and cyber defense within Israel's borders.

- It operates cyber units that focus on preventing terrorist use of cyberspace, detecting hostile cyber activities within the country, and securing government institutions against attacks. These units play a pivotal role in identifying online radicalization, thwarting cyber plots by terrorist organizations such as Hamas or Islamic Jihad, and monitoring domestic threats that involve cyber components. Shabak also collaborates with the Israel Police and INCD to protect public sector systems and critical civilian infrastructure from cyber intrusions and cyberterrorism.

- **The Ministry of Defense (MoD) Cyber and Technological Units** manages **research,** procurement, and development of cyber capabilities in collaboration with military and intelligence agencies. Through its Directorate of

Defense Research and Development (DDR&D, or MAFAT), the MoD funds and oversees cyber technology programs and dual-use platforms, often in coordination with the IDF and Mossad. It also handles security oversight of export-controlled cyber technologies and authorizes cyber-related arms deals under the Israeli Defense Export Control Agency (DECA). Although it does not conduct cyber operations directly, the MoD strategically builds and sustains national cyber capabilities through innovation, regulation, and industrial partnerships.

- **The Israel National Cyber Directorate (INCD)** is the primary civilian authority for national cybersecurity. Reporting directly to the Prime Minister's Office, the INCD is responsible for cybersecurity policy, coordination, protection of critical national infrastructure (CNI), and response to cyber incidents across the public and private sectors. It functions as Israel's CERT (Computer Emergency Response Team) and leads the development of national resilience through regulation, standards enforcement, and public-private partnerships. INCD also engages in international cyber diplomacy, capacity-building, and knowledge-sharing with allied countries. It does not perform offensive operations but ensures systemic protection and strategic coordination at the national level.

- **Israel Police National Cybercrime Unit (NCCU, Lahav 433)**, is the Israel Police's elite cyber law enforcement branch. While its primary mission is to investigate, prevent, and prosecute cybercrimes, including financial fraud, ransomware, child exploitation, darknet operations, cyberstalking, and politically motivated hacking, the NCCU also plays a vital role in combating cyberterrorism, working closely with Shabak and international agencies such as Europol and Interpol. The unit conducts digital analysis, arrests cybercriminals, and collaborates with technology companies to support legal surveillance and criminal investigations. It is crucial in bridging the operational gap between civilian law enforcement and national cyber intelligence.

5.6.3 Contracting Ecosystem

The Israeli cyber contracting ecosystem is a very powerful extension of its national cyber strategy. Many cybersecurity startups are spin-offs founded by veterans of Unit 8200 or Mossad's cyber teams, forming an innovation pipeline closely aligned with state needs. The Ministry of Defense, in collaboration with the Directorate of Defense Research and Development (DDR&D) and INCD, frequently contracts Israeli firms to develop surveillance tools, cyber-attack platforms, and advanced intrusion software. Companies like NSO Group, Cellebrite, CyberArk, and Check Point exemplify how private industry and government share resources, talent, and objectives. This partnership creates a dual-use ecosystem where tools developed for national

security also enter global markets, sometimes raising legal and ethical controversies, especially concerning spyware use. Moreover, the ecosystem benefits from Israel's robust venture capital environment, fostering rapid prototyping and deployment of cyber technologies.

5.6.4 Operational Objectives and Tactics

Israel's cyber operations are strategically designed to achieve multiple overlapping objectives: early warning, deterrence, disruption, and strategic surprise. Offensive cyber operations often aim to delay or disrupt adversarial capabilities, such as nuclear programs (e.g., Stuxnet, allegedly developed jointly with the U.S. against Iran), communications networks, and weapons systems. Tactics include advanced persistent threats (APTs), zero-day exploitation, ransomware-like disruption, data exfiltration, and even the psychological use of information operations. On the defensive front, Israel adopts a "digital Iron Dome" model, leveraging AI and real-time threat intelligence to detect and neutralize incoming attacks, especially against critical infrastructure like energy, finance, and water systems. The IDF has publicly acknowledged its willingness to respond to cyberattacks with kinetic force, establishing cyber deterrence through credible cross-domain escalation.

5.6.5 Target Profile and Geographical Focus

Israel's approach to cyber targeting is closely shaped by its complex geopolitical environment. At the forefront of its operations are regional adversaries—chiefly Iran, Hamas, Hezbollah, and Syria's military and intelligence apparatus. Iran remains Israel's highest-priority cyber target, owing to its advanced digital capabilities and pursuit of nuclear weapons. Israeli cyber units have reportedly been involved in operations against Iranian uranium enrichment facilities, command-and-control systems, and critical transportation and logistics networks. In addition to state-level threats, Israeli cyber efforts also extend to disrupting the digital infrastructure of terrorist organizations, conducting intelligence and influence campaigns against foreign government systems, and countering hostile media platforms. While the Middle East remains the core theater, Israeli cyber operations span a broader geographical spectrum, including Europe, North America, and Asia particularly in regions where Israeli diplomatic, security, or economic interests are at stake. Cyber capabilities have also been deployed in Africa and Latin America, either in collaboration with allied nations or to address specific threats such as arms trafficking, organized cybercrime, or transnational terrorism.

5.6.6 Evolution and Trends in Israel's Cyber Capabilities

Israel's cyber capabilities have evolved from reactive defense to predictive and preemptive dominance. Early reliance on passive defense has given way to machine learning-driven anomaly detection, automated threat hunting, and quantum-resilient encryption techniques. The IDF and INCD are integrating AI-enhanced cyber fusion

centers, capable of aggregating signals intelligence, human intelligence, and cyber data in real-time. Israeli cyber startups continue to pioneer sandbox evasion, zero-trust architectures, and next-gen endpoint detection and response (EDR) tools. Furthermore, Israel is actively investing in quantum computing research and post-quantum cryptography, anticipating the strategic implications of quantum breakthroughs. Another emerging trend is the fusion of cyber and electronic warfare (EW), allowing for synchronized attacks that blind, jam, and hack enemy networks simultaneously. The state's agile regulatory environment allows rapid testing and deployment, ensuring Israel stays at the cutting edge of cyber capability evolution.

5.7 US Cyber Strategy: Doctrine, Capabilities, and Operations

5.7.1 Strategic Overview of the United States' Cyber Activities

The United States' cyber strategy is embedded in its broader national defense and homeland security frameworks, emphasizing deterrence, resilience, and dominance in cyberspace. Facing constant threats from nation-states like China, Russia, Iran, and North Korea, as well as cybercriminal syndicates and non-state actors, the U.S. treats cyberspace as a domain of warfare equivalent to land, sea, air, and space. The Department of Defense (DoD), through its 2018 DoD Cyber Strategy and subsequent updates, prioritizes persistent engagement and defending forward, which include preemptive and retaliatory cyber operations. The U.S. Cyber Command (USCYBERCOM) leads this approach with integrated offensive and defensive capabilities. Civilian efforts are coordinated through the Cybersecurity and Infrastructure Security Agency (CISA), which focuses on protecting critical infrastructure and supporting public-private partnerships. U.S. cyber strategy also includes cyber diplomacy, supply chain security, and coalition-building through frameworks like the Five Eyes alliance and NATO cyber defense policy.

5.7.2 United States' Cyber Power: Key Institutions and Structures

The United States arguably has the most military and civilian cyber entities. With a colossal budget, the country has developed a mighty and sophisticated cyber structure with multiple agencies and cyber units, including the following:

- **The U.S. Cyber Command (USCYBERCOM)** is the central military command responsible for coordinating cyber operations across all branches of the U.S. military. Under the DoD, USCYBERCOM executes offensive cyber operations, defends military networks, and supports combatant commanders globally. Its dual-hatted commander also leads the National Security Agency (NSA), enabling seamless integration between signals intelligence and the army cyber operations.

- **The NSA Cybersecurity Directorate** focuses on securing national security systems and collaborates with USCYBERCOM on both defensive and offensive cyber operations. The NSA's elite **Tailored Access Operations (TAO)** team conducts some of the world's most sophisticated cyber-espionage and offensive missions, targeting adversary infrastructure, military networks, and leadership communications.
- **The Department of Homeland Security (DHS) CISA** is the United States' lead civilian agency for cybersecurity. CISA coordinates the protection of federal civilian executive branch systems and partners with the private sector to defend critical infrastructure sectors such as energy, healthcare, and finance.
- **The National Cybersecurity and Communications Integration Center (NCCIC)**, acts as a national fusion center for cyber threat intelligence and incident response.
- **The Federal Bureau of Investigation (FBI)** Cyber Division investigates cybercrime, counterintelligence threats, and terrorist cyber activity. It leads the National Cyber Investigative Joint Task Force (NCIJTF), which coordinates federal efforts in attribution, law enforcement operations, and the disruption of cyber actors.
- **The Central Intelligence Agency (CIA) Center for Cyber Intelligence (CCI)** conducts cyber-espionage, offensive cyber operations, and influence campaigns abroad. The CIA operates covert cyber units tasked with long-term infiltration of foreign systems and clandestine digital sabotage in support of U.S. foreign policy goals.
- **The National Security Council (NSC)** and the **Office of the National Cyber Director (ONCD)**, reporting to the White House, are responsible for cyber policy coordination, national strategy formulation, and interagency synchronization of cyber-related efforts.

5.7.3 Contracting Ecosystem

The U.S. cyber contracting ecosystem is expansive, driven by both defense procurement and commercial innovation. Defense contractors such as Raytheon, Lockheed Martin, Northrop Grumman, and Booz Allen Hamilton play significant roles in cyber tool development, network defense, and operations support for agencies like USCYBERCOM and NSA. In the commercial sector, companies like CrowdStrike, FireEye (now Trellix), Palo Alto Networks, and Mandiant are industry leaders in threat detection and incident response. The Silicon Valley and other innovation hubs contribute significantly to U.S. cyber capabilities through startup accelerators, venture capital investment, and DARPA-funded research.

Technologies developed under government contracts often have dual-use potential, with military and civilian applications. This ecosystem is reinforced by federal funding initiatives like In-Q-Tel, which invests in emerging technologies relevant to the intelligence community.

5.7.4 Operational Objectives and Tactics

The U.S. cyber operations serve to deter, disrupt, degrade, and, when necessary, destroy adversarial cyber capabilities. Offensive operations are guided by principles such as defend forward and persistent engagement, meaning the U.S. proactively engages adversaries in their own networks to prevent attacks before they reach U.S. soil. These operations may involve malware deployment, infrastructure disruption, and influence campaigns, as seen in the takedowns of ISIS propaganda networks and ransomware infrastructure. Defensive efforts prioritize critical infrastructure resilience, public-private threat intelligence sharing (e.g., Joint Cyber Defense Collaborative), and rapid incident response. The U.S. also reserves the right to respond to major cyberattacks with conventional or nuclear force, establishing deterrence across multiple domains.

5.7.5 Target Profile and Geographical Focus

Primary adversaries include China (cyberespionage and intellectual property theft), Russia (information warfare and infrastructure attacks), Iran (regional destabilization and cyberterrorism), and North Korea (financial cybercrime and strategic disruption). U.S. cyber units frequently target command-and-control servers, military systems, hacker infrastructures, and adversarial propaganda outlets. The global reach of the United States' cyber operations spans from Europe and the Indo-Pacific to the Middle East and Latin America. Strategic allies often cooperate with U.S. cyber forces through joint operations or intelligence sharing, particularly within NATO, the Five Eyes, and regional security pacts.

5.7.6 Evolution and Trends in the United States' Cyber Capabilities

U.S. cyber capabilities continue to evolve toward autonomous, AI-driven threat detection and preemptive response. Advanced persistent threat (APT) detection, behavioral analytics, and quantum-safe cryptography are rapidly being adopted. The DoD invests heavily in zero-trust architecture, multi-domain command-and-control (JADC2) integration, and cyber-electromagnetic activities (CEMA) that merge EW and cyber operations. The USCYBERCOM and DARPA are leading initiatives in post-quantum cryptography, offensive cyber AI, and resilient satellite communications. The fusion of cyber and space operations is an emerging focus, especially with the establishment of the U.S. Space Force and its cyber components. Policy developments emphasize supply chain security (e.g., Executive Order 14028), open-source software integrity, and domestic cyber workforce expansion to maintain U.S. dominance in cyberspace.

Chapter 7: Disinformation and Information Warfare

7.1 The Strategic Evolution of Disinformation in the Cyber Domain

Disinformation has become a central pillar of 21st-century conflict, evolving from traditional state propaganda into a sophisticated, cyber-enabled tool of geopolitical influence and asymmetric warfare. In the past, information warfare was constrained mainly by geographical, linguistic, and technological limitations, often relying on controlled media channels, clandestine leaflets, or limited radio broadcasts. Today, however, the proliferation of digital platforms, artificial intelligence, and anonymizing tools has obliterated those boundaries, enabling malign actors to reach global audiences instantly and with minimal attribution risk. What once required significant state infrastructure and manpower can now be achieved by a small, well-coordinated group operating anywhere in the world.

Modern disinformation campaigns are not merely psychological operations (PSYOPs); they are complex, multi-layered strategies that exploit digital ecosystems to destabilize societies, undermine trust in institutions, and erode the cognitive sovereignty of target populations. These operations often integrate cyberattacks, social engineering, and behavioral analytics to tailor disinformation content to specific demographics, amplifying its psychological impact and polarizing public discourse. Nation-states and non-state actors alike now weaponize information with surgical precision, leveraging bots, troll farms, deep fakes, and selectively released or fabricated content to blur the line between truth and falsehood. The aim is not always to persuade, but often to confuse, demoralize, or paralyze creating a fragmented information landscape where objective reality becomes contested and consensus impossible.

Importantly, disinformation is a force multiplier in hybrid warfare, enabling adversaries to shape narratives, sow discord, and exert strategic pressure without crossing conventional military thresholds. Russia’s interference in Western elections, China’s disinformation during the COVID-19 pandemic, and the Islamic State’s online radicalization campaigns exemplify the diverse motivations and methods behind these efforts. Moreover, the increasing use of artificial intelligence to generate realistic fake content such as synthetic voices, images, and videos—portends a future where detecting manipulation will become exponentially more difficult, even for experts.

This chapter examines disinformation campaigns' geopolitical, strategic, and technological aspects, drawing from contemporary case studies and intelligence assessments to illustrate their scale, effectiveness, and implications for national security. It argues that countering disinformation requires technical solutions, such as algorithmic detection and platform regulation, and a societal response that includes digital literacy, institutional transparency, and international norms for information integrity. As the information domain becomes increasingly contested, understanding and mitigating the threat of disinformation is vital for safeguarding democratic resilience and global stability.

7.2 Geopolitical Motives and State Actors

Using disinformation in cyberspace is often an extension of statecraft—a continuation of foreign policy by other means. Major geopolitical players like Russia, China, and Iran have institutionalized information warfare as a component of their military doctrines. Russia's Gerasimov Doctrine explicitly embraces the fusion of military and non-military tools, including media manipulation, social media disruption, and cyber-enabled psychological operations, to achieve strategic objectives. The Kremlin's campaigns, such as those surrounding the 2016 U.S. presidential election, the Brexit referendum, and conflicts in Ukraine,e have been characterized by the deliberate spread of conflicting narratives aimed at amplifying societal divisions and discrediting democratic norms. Similarly, China's Three Warfares strategy, comprising public opinion warfare, psychological warfare, and legal warfare,e places significant emphasis on the control and distortion of narratives to expand its global influence. Through state-run media, coordinated influencer campaigns, and digital surveillance, Beijing has executed disinformation efforts to shape perceptions around issues like the COVID-19 pandemic, Hong Kong protests, and the status of Taiwan. Unlike Russia's often chaotic and overtly disruptive style, China prefers a subtle, long-term erosion of trust through selective amplification and censorship. These approaches reveal differing strategic cultures and diverse operational models tailored to specific geopolitical objectives.

7.3 Cyber Infrastructure and the Weaponization of Platforms

Disinformation campaigns operate across a complex cyber infrastructure encompassing overt public platforms and covert communication channels. Social media sites such as Facebook, X (formerly Twitter), YouTube, and TikTok are primary vectors for distributing misleading content. These platforms are particularly vulnerable due to their massive scale, the prioritization of engagement over factual accuracy, and their reliance on algorithmic amplification. Malicious actors exploit these structural weaknesses through coordinated inauthentic behavior (CIB), employing fake personas, sockpuppet accounts, and botnets to simulate genuine user activity and organic discourse.

Increasingly, artificial intelligence is used to create compelling fake profiles, complete with fabricated images and misleading content (Figures 54 and 55). These tools not only spread falsehoods but also manipulate trending topics, harass dissenters, and reinforce echo chambers. Beyond social media, encrypted messaging apps like Telegram and Signal, along with dark web forums, offer secure environments for coordination and dissemination beyond the reach of content moderators and law enforcement. Nation-state actors often obscure their involvement through front organizations and third-party proxies, maintaining plausible deniability. This weaponization of digital platforms extends further into search engines, recommendation systems, and even voice assistants, transforming everyday digital interactions into persistent avenues for psychological and informational manipulation.



Figure 54 - AI-generated image posted by suspected Chinese IO assets (Source: Microsoft)

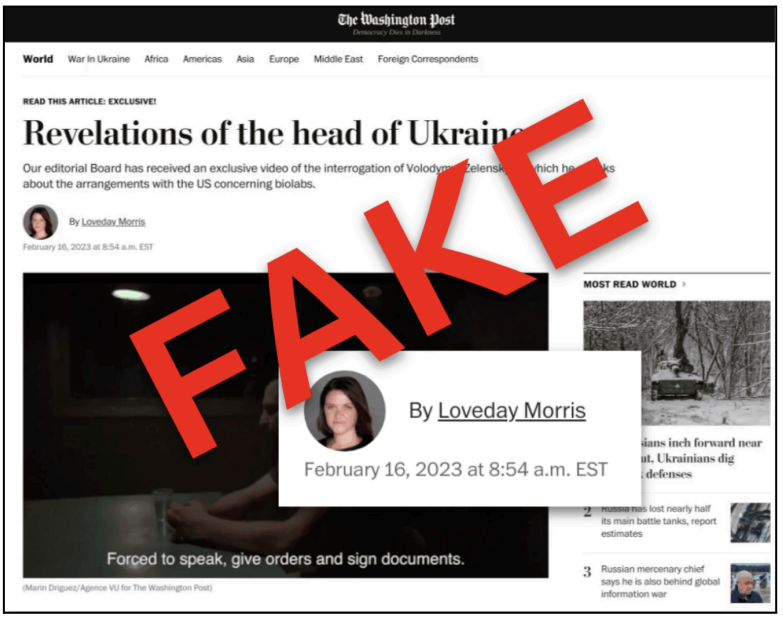


Figure 55 - An example of a fake article created by Russia and impersonating the Washington Post (Source: Meta)

7.4 Tactics, Techniques, and Procedures (TTPs)

The deployment of disinformation relies on a sophisticated suite of Tactics, Techniques, and Procedures (TTPs) crafted to manipulate perception and destabilize societies. These operations exploit information and imagery, often using fear, denial, and denigration to achieve psychological influence (Figure 56). One prominent method is narrative laundering, where false or misleading claims are introduced through obscure or foreign sources and gradually amplified by more credible outlets until they are accepted as truth. Astroturfing creates the illusion of grassroots support by staging fake petitions, protests, or viral content, manufacturing consensus where none exists. False flag operations further obscure attribution by disguising the true origin of campaigns, often to incite geopolitical tension or discredit adversaries. More advanced disinformation tools include deepfakes, highly realistic AI-generated audio or video designed to impersonate public figures, spread falsehoods, or sow confusion. Cyber-enabled leaks involve the strategic release of hacked materials, selectively framed to support misleading narratives. These techniques are frequently timed to coincide with pivotal events such as elections, referendums, or international summits. They often coordinate with diplomatic, economic, or military actions to amplify their strategic effect. This level of orchestration exemplifies the convergence of hybrid warfare and strategic communication, where cyber operatives, media technicians, and geopolitical planners work in concert to shape global narratives.

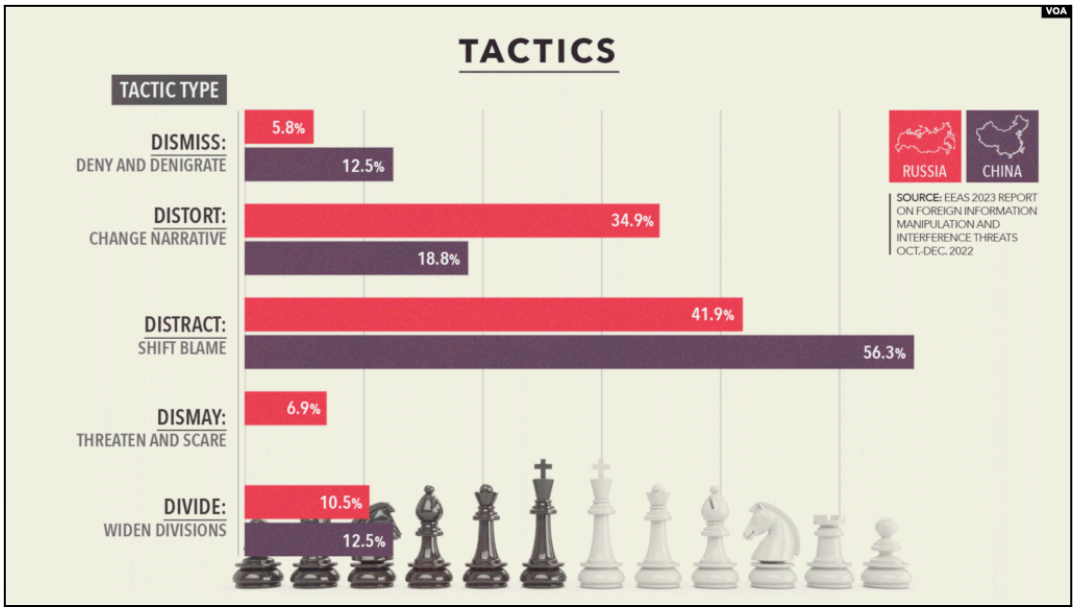


Figure 56 – Tactics used by Russia and China in disinformation campaigns (Source: VOA)

7.5 The Psychological and Societal Impact

At its core, disinformation warfare is a cognitive assault. Its primary target is not infrastructure but perception, aiming to fragment shared reality, exhaust critical thinking, and induce what has been called “epistemic nihilism,” where audiences cease to believe in the possibility of objective truth. The effects are profound: electoral processes are delegitimized, public health responses are undermined, and social cohesion deteriorates. Disinformation campaigns often exploit preexisting cultural, ethnic, or political fissures, magnifying them into crises of identity and governance. They foster polarization by promoting hyper-partisan narratives, conspiracy theories, and anti-institutional sentiments. Importantly, the impact is not confined to the digital realm it manifests in real-world violence, civil unrest, and diplomatic breakdowns. The feedback loop between online manipulation and offline consequences presents a growing threat to democratic resilience, especially in nations with high digital penetration and low media literacy. Even when disinformation is eventually debunked, the “illusory truth effect” ensures that repeated exposure can reinforce belief, making post hoc corrections largely ineffective. This asymmetry, where attackers need only to plant seeds of doubt while defenders must painstakingly counter them, renders disinformation an ideal weapon for asymmetric conflict.

7.6 Detection, Attribution, and Countermeasures

Efforts to detect and counter disinformation are advancing, but the challenges remain formidable. Machine learning and natural language processing tools have been developed to identify coordinated behavior and textual anomalies, but adversaries continuously adapt, leveraging generative AI and linguistic camouflage to evade detection. Attribution is particularly difficult; while indicators like IP addresses, language patterns, and metadata can suggest culpability, sophisticated actors obfuscate these trails through proxies, VPNs, and false-flag tactics. As a result, effective countermeasures require a fusion of cyber forensics, open-source intelligence (OSINT), and geopolitical analysis. On the policy front, some governments have introduced legislation to increase transparency in political advertising, regulate platform algorithms, and impose sanctions on foreign disinformation entities. However, these efforts are often stymied by concerns over free speech, technological jurisdiction, and international cooperation. Civil society also plays a critical role through fact-checking networks, media literacy programs, and digital hygiene campaigns. The private sector, particularly social media platforms, has made incremental progress through content moderation, AI-driven filtering, and threat reporting. Still, these efforts are uneven and often reactive rather than preventive. Ultimately, the defense against disinformation must be comprehensive and multidisciplinary, encompassing technology, law, diplomacy, and education.

7.7 The Future Trajectory of Information Warfare

Looking ahead, the trajectory of disinformation warfare points toward greater scale, automation, and personalization. Generative AI technologies will enable the rapid creation of hyper-realistic fake content tailored to specific psychological profiles, thereby increasing the persuasive power of campaigns. Predictive analytics and behavioral microtargeting, already used by marketing firms and political operatives, will be weaponized to deliver emotionally resonant and ideologically calibrated messages that bypass rational scrutiny. The emergence of the metaverse and extended reality (XR) platforms introduces new domains where immersive disinformation can take root, manipulating perception through synthetic environments and avatars. Meanwhile, quantum computing and 6G networks could accelerate the dissemination and obfuscation of disinformation beyond current detection capabilities. Geopolitically, we may see the formation of “information alliances,” wherein nations coordinate their disinformation strategies or establish digital influence spheres analogous to Cold War-era blocs. Conversely, new international norms and cyber treaties may emerge to develop rules of engagement and liability in the information domain. The central challenge for policymakers, technologists, and society will be to defend the epistemological integrity of the public sphere without undermining democratic freedoms—a task that demands vigilance, innovation, and cross-sectoral collaboration.

Chapter 8: Cyberterrorism and Hacktivism

8.1 Introduction to Cyberterrorism

Cyberterrorism can be broadly defined as the use of information and communication technologies by terrorist actors to instill fear, exert political or ideological influence, or disrupt critical national infrastructure. These activities often target civilian populations and state institutions, leveraging the digital environment's anonymity, reach, and low-cost nature. First discussed in the early 1990s, cyberterrorism began to emerge as a serious concern in the 2000s, and by the 2010s, it had evolved into a significant dimension of modern security discourse. As a concept, cyberterrorism must be clearly distinguished from related but distinct phenomena such as hacktivism and cyberwarfare. Hacktivism generally involves non-violent, politically motivated cyber activities such as website defacement or digital protests to promote a cause. Cyberwarfare, by contrast, is typically conducted by nation-states during periods of conflict and often involves strategic disruption of enemy infrastructure. However, cyberterrorism occupies a unique space wherein non-state actors adopt digital tools to pursue ideological agendas, incite fear, or cause large-scale disruption and destruction.

The growth of cyberterrorism is closely linked to the exponential expansion of cyberspace and the increasing digitalization of national infrastructures. Contemporary societies depend heavily on interconnected systems for essential services ranging from energy grids and water supplies to healthcare systems and financial networks. Terrorist organizations have recognized this vulnerability and adapted accordingly, embedding cyber capabilities into their operational structures. For some analysts, cyberterrorism simply extends traditional terrorism into the digital domain; for others, it constitutes a fundamentally new threat paradigm.

The appeal of cyberspace to terrorist actors lies in several key advantages. First, cyber operations are generally less costly than traditional physical attacks and can be conducted remotely, reducing the risk of detection or interception. Encryption technologies and anonymizing tools further enhance the ability of terrorists to operate covertly. Moreover, cyberterrorism allows for a potentially broader scope of impact, enabling actors to simultaneously target multiple institutions across borders. Despite occasional high-profile physical attacks carried out with minimal resources, it is essential to note that executing sophisticated cyberattacks, especially those capable of disrupting state functions, often requires considerable technical skill and financial investment. Nevertheless, the strategic value of cyber capabilities has led many terrorist groups to invest in building dedicated cyber units. These may consist of technically trained members or external recruits, including professional hackers motivated by ideological or financial incentives. Today, the functions of cyberspace within terrorist operations are multifaceted. These include:

- **Propaganda dissemination** aimed at shaping public opinion and radicalizing audiences
- **Psychological warfare** through symbolic digital attacks or threats
  Recruitment of sympathizers via social media and encrypted platforms
- **Training and knowledge sharing** through manuals, video content, and dark web forums
- **Fundraising**, including through cryptocurrencies, online fraud, and crowdfunding
- **Intelligence gathering** from open sources or through illicit data access
  Secure communication to coordinate activities across dispersed locations
  Cyberattacks, such as distributed denial-of-service (DDoS), malware deployment, data theft, and defacement of websites

Unlike conventional criminal organizations that exploit cyberspace primarily for financial gain, terrorist groups weaponize the digital domain to advance extremist ideologies and destabilize governments. Recognizing the strategic power of the internet, many such groups have incorporated cyber tactics into their long-term operational strategies. Over the past decade, this trend has accelerated, transforming cyberterrorism from a theoretical concern into a concrete and evolving threat to international security.

8.2 Cyber Terrorism and Radical Islamist Organizations

The evolution of the Internet and the widespread adoption of social media platforms have fundamentally transformed political and religious activism worldwide. Initially pioneered by hacktivist groups such as Anonymous, digital technologies quickly became powerful tools for various ideological movements, including radical Islamist organizations. These groups have adeptly leveraged cyberspace to spread propaganda, recruit new members, coordinate operations, and amplify their messages on a global scale. For many Muslims globally, cyberspace has become a critical source of information and communal interaction, even though some content and behaviors online may contradict traditional Islamic ethics. This digital engagement surged during the Arab Spring of 2011, when social media platforms were pivotal in mobilizing protests, disseminating real-time updates, and attracting international attention to the unfolding political upheavals. In this era, digital communication was widely perceived as an instrument of liberation and empowerment. However, the aftermath of the Arab Spring also saw increased civil unrest and a troubling rise in radicalization. Terrorist organizations with radical Islamist ideologies seized the opportunity to expand their digital footprint. The concept of “cyber jihad” emerged as an extension of traditional jihadist activity into the virtual realm. Groups such as the Islamic State (ISIS) developed sophisticated online strategies to propagate their ideology and recruit followers globally. The success of these cyber strategies depends heavily on the organization’s technical expertise, ability to attract and train hackers, and financial resources.

As of 2025, the financial strength of these organizations remains a decisive factor in developing their cyber capabilities. According to the latest analyses, the Taliban is currently the wealthiest terrorist organization, with estimated annual revenues nearing $2.5 billion, primarily derived from drug taxation and illicit mining operations. The Houthi rebels in Yemen closely follow, generating around $2 billion annually through control of local economies and illegal oil trade. Hamas earns approximately $500 million per year through taxation in Gaza and external support, while Al-Qaeda sustains about $300 million through smuggling and taxation in controlled areas. Although diminished in territorial control, ISIS still accrues roughly $200 million annually from illegal oil sales and other illicit activities. These considerable financial resources enable these groups not only to sustain traditional operations but also to expand and enhance their cyber warfare and propaganda capabilities, posing significant ongoing challenges to global security and counterterrorism efforts. The following image (Figure 57) illustrates the primary Islamist terrorist organizations based on their estimated financial strength and cyber influence as of 2025.



Figure 57 - Flags of the leading Islaist terrorist organizations

8.3 Use of Cyberspace by Radical Islamist Organizations

Radical Islamist terrorist organizations have become increasingly sophisticated in exploiting the multiple layers of cyberspace to advance their strategic goals, including recruitment, propaganda dissemination, intelligence gathering, and operational coordination. Their use of cyberspace can broadly be categorized into three main domains: social networks, encrypted messaging applications, and the darknet. Each layer offers unique opportunities and challenges, and terrorist groups continuously adapt their digital tactics to evade counterterrorism efforts, maximize outreach, and enhance operational security.

8.3.1 Social Networks

Social networks remain the most accessible and widespread digital platforms globally, boasting billions of active users and serving as powerful vehicles for communication and influence. Hosted on publicly accessible servers and easily discoverable through traditional search engines, these platforms provide terrorist organizations unparalleled reach. Over the past decade, the proliferation of niche social networks, multilingual platforms, and multimedia sharing sites has broadened the digital landscape. This abundance allows Islamist terrorist groups to create diverse online ecosystems tailored to different audiences and languages.

In many Middle Eastern countries, platforms such as Facebook, WhatsApp, and Instagram dominate, providing fertile ground for terrorist propaganda and communication. Groups such as Hamas, Hezbollah, and ISIS have established official and unofficial social media pages, using them to claim responsibility for attacks, disseminate ideological content, and recruit sympathizers. These groups often employ community managers who curate content daily, ensuring a continuous flow of propaganda and engagement. For example, Hamas' military wing frequently posts on Instagram, showcasing its operations and rallying support (Figure 58).

Similarly, the Jerusalem Electronic Army maintains active Facebook and Instagram pages to coordinate cyber activities and propagate its narrative (Figures 59 and 60).



Figure 58 - An Instagram post by Hamas' military wing claiming responsibility for an attack against Israel



Figure 59 – The Facebook page of the Jerusalem Electronic Army

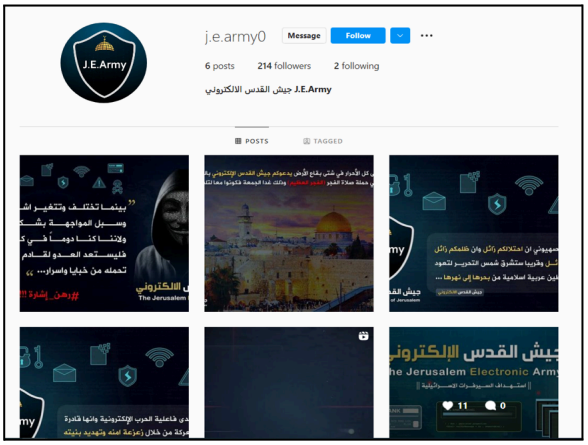


Figure 60 - The Instagram page of the Jerusalem Electronic Army

Beyond propaganda, social networks serve as a virtual battlefield for cyber intelligence operations. Hamas, for instance, has mastered the use of fake profiles often posing as attractive young women (Figure 61) to establish trust with Israeli soldiers via private messaging. Once contact is made, they lure targets into clicking malicious links that install spyware, allowing terrorists to collect sensitive data such as geolocation, messages, and call logs. This tactic illustrates how human vulnerabilities are exploited for cyber intelligence gathering with relatively low technological investment but high operational payoff. These social networks, thus, act as multifunctional tools combining psychological operations, recruitment, and cyber espionage.

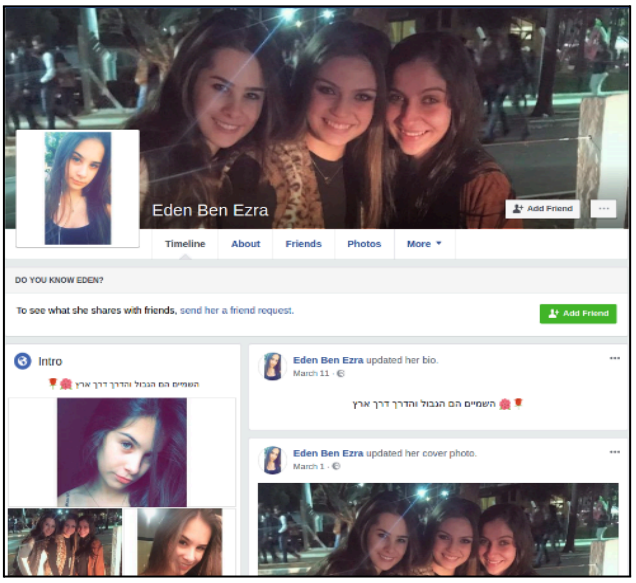


Figure 61 - Hamas' fake Facebook profile created for luring Israeli soldier

8.3.2 Encrypted Messaging Applications

As global surveillance and counterterrorism technologies become increasingly sophisticated, terrorist organizations have evolved in parallel turning to encrypted messaging applications as a critical component of their digital operations. These platforms offer end-to-end encryption, metadata obfuscation, and decentralized hosting capabilities, allowing extremist groups to communicate securely, recruit new members, coordinate attacks, transfer funds, and disseminate propaganda with minimal risk of exposure. The following encrypted messaging applications are or were the most popular among terrorist organizations. The following table summarises all their different features (Figure 62).



Encrypted Messaging Applications Used by Terrorist Organizations (2025)

Application	Encryption	Anonymity	Group/Broadcast Features	Server Model	Known/Reported Use by Terrorist Groups
WhatsApp	✅ End-to-end	❌ Requires phone number	⚠️ Limited broadcast	Centralized	Early use by jihadist groups; now less favored due to traceability (Gartenstein-Ross, 2018)
Telegram	⚠️ Not E2E by default	✅ With prepaid SIMs	✅ Large channels/groups	Centralized	Widely used by ISIS, Hamas, Hezbollah; key platform for propaganda (Weimann, 2016; Vox, 2025)
Rocket.Chat	⚠️ Optional E2E	✅ Fully anonymous with self-hosting	✅ Full group support	Decentralized/self-hosted	Used by ISIS and Al-Qaeda affiliates for propaganda and planning (Clifford & Powell, 2019)
Signal	✅ End-to-end	❌ Requires phone number	🚫 Limited group capacity	Centralized	Recommended for 1-on-1 secure chats by jihadist guides; limited adoption for large operations
Threema	✅ End-to-end	✅ No phone/email needed	⚠️ Moderate group tools	Centralized (Swiss)	Used by extremist cells in India and Europe for secure comms (NCRI, 2020)
SimpleX Chat	✅ End-to-end	✅ No phone/email/account	⚠️ Developing group tools	Decentralized	Adopted by far-right extremists fleeing Telegram in 2025 (Wired, 2025)
Session	✅ End-to-end via onion routing	✅ No registration/metadata	✅ Group support	Decentralized (Oxen)	Used by ISIS-aligned groups, including Electronic Horizon Foundation
Tox Protocol	✅ End-to-end	✅ Fully decentralized, no servers	⚠️ Complex group setup	Peer-to-peer	Niche but attractive to tech-savvy cells avoiding server-based tools
Briar	✅ End-to-end (mesh networking)	✅ No internet required	⚠️ Small local groups only	Offline/mesh	Used in field ops in high-surveillance or disconnected zones

🔍 **Legend:**

- ✅ = Strong support or feature
- ⚠️ = Limited or optional capability
- ❌ = Weak or absent feature
- E2E = End-to-end encryption

Figure 62 - Encrypted messaging apps used by terrorist organization

- **WhatsApp** was among the first widely adopted encrypted platforms used by jihadist and militant groups due to its accessibility and reliable end-to-end encryption. However, its mandatory phone number registration and account-linking requirements limit anonymity and operational security. Consequently, many groups have transitioned to platforms offering stronger identity protection and less central oversight.

- **Telegram** continues to be one of the most actively used platforms by terrorist and extremist groups due to its robust broadcast features, user anonymity (via prepaid SIM registration), and weak content moderation. Channels affiliated with Hamas's Izz ad-Din al-Qassam Brigades, Hezbollah, and ISIS-linked media outlets routinely share operational messages, manuals, and propaganda on Telegram (Figure 63).

Despite increasing legal and political pressure, including the 2025 detention of CEO Pavel Durov in France,Telegram remains resilient, and groups like ISIS and neo-Nazi networks under the Terrorgram umbrella have persisted on the platform.

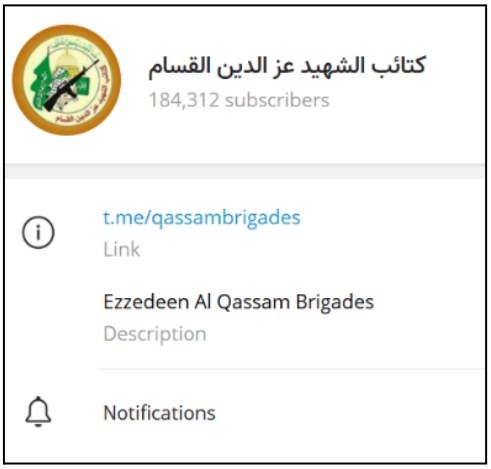


Figure 63 - The Ezzedeen Al Qassam Brigades' Telegram Channel

- **Signal** has become a preferred communication tool for some terrorist organizations due to its strong end-to-end encryption, minimal data retention, and disappearing message features, providing high operational security. Unlike platforms with public broadcast capabilities, Signal is mainly used for private, encrypted conversations, making it attractive for coordinating attacks, recruitment, and sharing sensitive information without risk of interception. Groups linked to ISIS, al-Qaeda, and other extremist networks have been reported to adopt Signal for secure internal communications, exploiting its anonymity and resistance to surveillance. Despite efforts by governments to monitor encrypted communications, Signal's privacy-first design continues to pose significant challenges to counterterrorism operations.
- **Rocket. Chat, an open-source**, self-hosted communication platform, has been deployed by ISIS and Al-Qaeda affiliates for secure, encrypted group chats since 2018–2019. Its customizable architecture allows groups to run private servers without depending on external infrastructure, minimizing the chance of surveillance or takedown (Figure 64).

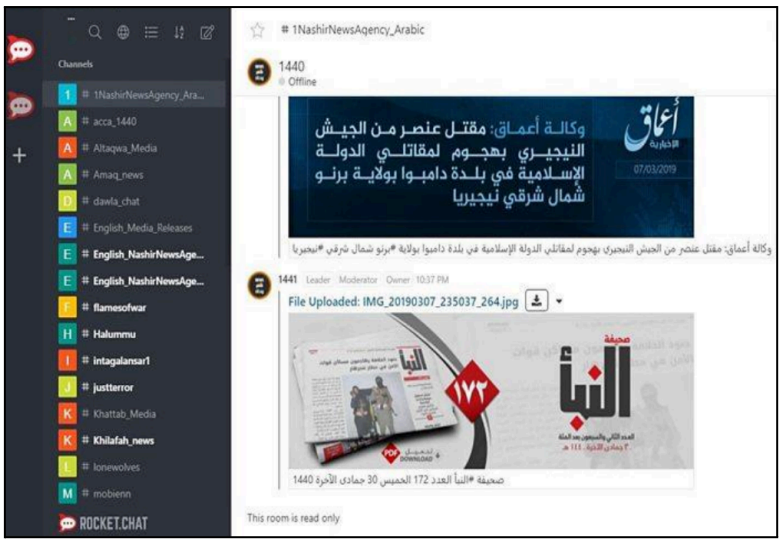


Figure 64 - The Nashir News Agency broadcasting Islamic State propaganda on RocketChat

- **Threema,** developed in Switzerland, offers strong privacy protections, including registering without a phone number or email. It has reportedly been used by jihadist cells in India and elsewhere in South Asia, drawn by its security-conscious design and European jurisdiction, which is seen as less susceptible to extrajudicial data demands

- In 2025, **SimpleX Chat** emerged as a migration destination for far-right extremist actors leaving Telegram in the wake of arrests and digital disruption campaigns targeting the Terrorgram network. SimpleX's key features, including metadata minimization, lack of account credentials, and decentralized message delivery, make it attractive to groups seeking enhanced anonymity.

- **Session** has become a notable platform for extremist groups due to its use of onion routing (via the Oxen network) and lack of centralized servers. The app enables pseudonymous messaging without requiring user registration, phone numbers, or emails. These features reduce the risk of surveillance and are aligned with the technical preferences of jihadist cyber divisions like ISIS's Electronic Horizon Foundation.

- **Tox Protocol** provides end-to-end encryption over a decentralized, peer-to-peer network, eliminating any central servers that authorities might compromise. While still niche, its robustness makes it appealing to tech-savvy cells looking to avoid server-based vulnerabilities.

- **Bria** uses Bluetooth and Wi-Fi-based mesh networking to allow encrypted communications without internet access. This makes it a vital tool for terrorist groups operating in disconnected or heavily surveilled regions. Briar is especially useful for coordinating field operations in conflict zones or during blackouts.

- **EncroChat and Ciphr:** Beyond mainstream apps, terrorist networks and organized crime groups have also used purpose-built encrypted devices such as EncroChat and Ciphr. Though both were ultimately dismantled by European law enforcement, their widespread use highlights demand for high-grade encryption in criminal and extremist circles. Their downfall also pushed groups to seek more decentralized solutions.

8.3.4 Darknet

By 2025, the darknet, particularly the Tor (The Onion Router) network, will continue to play a pivotal role in the digital operations of radical Islamist organizations. Its underlying architecture, characterized by layered encryption and decentralized routing, offers robust protection against surveillance and censorship, making it an enduring refuge for illicit activity. While encrypted messaging platforms and mainstream social media remain essential tools for broad propaganda dissemination, the darknet provides a more secure and resilient environment for hosting extremist websites, discussion forums, and repositories of sensitive materials that would be swiftly removed from the surface web. Organizations like the Islamic State have long relied on Tor-based infrastructure to distribute official communiqués, ideological treatises, and strategic documents, capitalizing on the darknet's anonymity and resistance to takedowns (Figures 65 and 66). In addition to propaganda dissemination, darknet marketplaces and forums facilitate the trade of weapons, forged identification documents, and cybercrime services, thereby enabling terrorist groups to sustain themselves financially and logistically.

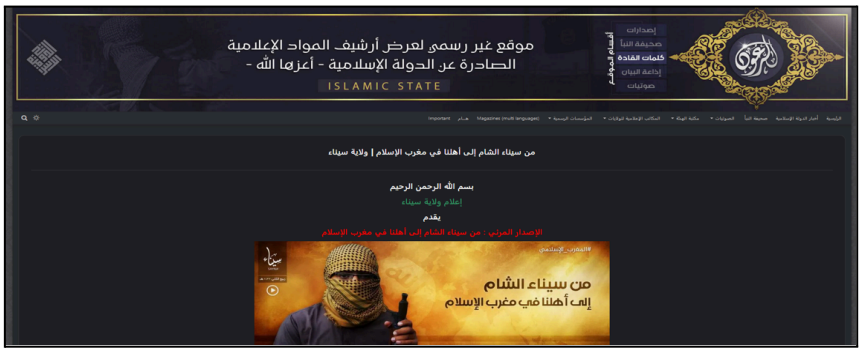


Figure 65 - A hosted TOR website broadcasting ISIS announcements and ideology (Source: dark web)



Figure 66 - A hosted TOR website broadcasting ISIS announcements and ideology (Source: dark web)

As of 2025, intelligence services continue to monitor key jihadist sites such as Maktabat al-Jihad 3.0, a comprehensive digital library containing translated ideological texts, tactical manuals, and multimedia training resources. These materials are frequently mirrored on decentralized file-sharing platforms to ensure their persistence even when primary hosting is disrupted. Furthermore, darknet forums enable anonymous exchanges on operational security techniques, including methods for evading facial recognition technologies and metadata surveillance. In this sense, the darknet has evolved beyond a tool for propaganda; it now functions as a dynamic hub for tactical innovation and secure coordination. Though its reach is more limited and specialized than that of mainstream platforms, the darknet remains an indispensable component of the digital infrastructure supporting modern jihadist networks.

8.4 Key Terrorist Organizations and Their Cyber Activities

8.4.1 Hamas

Over the past decade, Hamas has developed and expanded its offensive cyber capabilities, primarily targeting Israel, occasionally the United States, and specific Palestinian entities. These operations are heavily focused on cyber espionage and intelligence gathering, supporting strategic decision-making and military planning. At the core of these efforts is Hamas's intelligence apparatus, which draws personnel from the al-Majd security forces, a subdivision of the Izz al-Din al-Qassam Brigades, Hamas's military wing. Hamas's cyber operations have evolved in both scope and sophistication. In the early 2010s, its campaigns relied on mass-distributed phishing emails with malicious attachments. Over time, the group adopted more targeted techniques, including link-based malware delivery and advanced social engineering tactics such as using fake Facebook profiles to lure Israeli soldiers into installing spyware on their smartphones.

While the majority of Hamas's cyber activity remains focused on intelligence collection, the group also engages in cyberattacks aimed at data breaches, public leaks, and psychological manipulation. Notable incidents include claimed intrusions into organizations such as Cellcom, Egged, and Israel Aerospace Industries (IAI). Additionally, Hamas has employed DDoS attacks and website defacements to disrupt services and disseminate propaganda.

Organizational Structure and Cyber Division

Hamas' cyber operations are closely tied to the intelligence wing of its military arm, the Izz al-Din al-Qassam Brigades, and supported operationally by al-Majd, Hamas' internal security force. This organizational structure ensures that cyber efforts align directly with the group's military and political goals. According to disclosures made by Hamas in 2022, its dedicated cyber unit, " Izz ad-Din al-Qassam Cyber Fighters," has been active since 2014. It was founded by Juma al-Tahla, a senior commander later killed during the 2021 Gaza conflict.

The group's cyber strategy is multifaceted. It includes:

- Cyber espionage for strategic intelligence.
- Information warfare to erode public trust.
- Psychological operations often target civilians and soldiers.
- Hacktivism and defacement are used for propaganda and morale impact.
- Denial-of-service attacks as digital disruption tactics.

Evolution of Cyber Capabilities (2012–2025)

Early Period (2012–2016): Basic Techniques and Social Engineering

Initial operations were characterized by phishing attacks and crude malware distributed via mass email campaigns. Social engineering soon emerged as a core tactic, particularly against Israeli Defense Forces (IDF) personnel. Facebook and WhatsApp were exploited to distribute spyware disguised as legitimate software or personal interactions. Notably,

- In 2012, Hamas claimed to have disrupted the IDF's Home Front Command website, and in 2013, affiliated actors launched a DDoS attack against American Express, signaling broader intent beyond regional targets.

Maturing Tactics (2017–2021): Strategic Targeting and Hybrid Campaigns

- In 2018, Hamas had refined its social engineering tactics to include fake personas, often posing as attractive women, to lure IDF soldiers into downloading infected applications. A malicious imitation of the "Red Alert" app used by Israeli civilians to track incoming rocket warnings demonstrated the group's intent to exploit civil defense tools (Figure 67). Operations also expanded to regional political espionage.

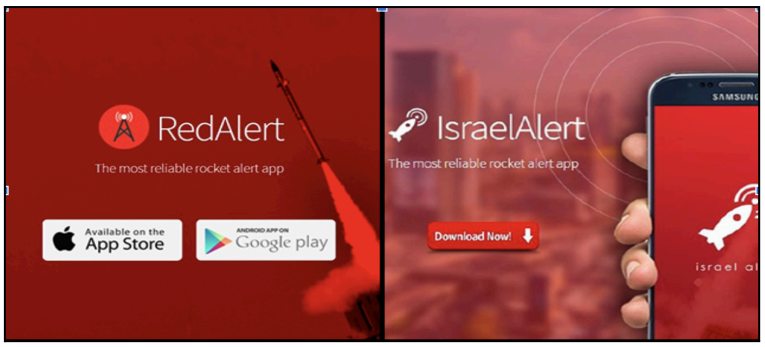


Figure 67 - On the left, the real app and on the right, the fake Red Alert app

- In 2019, the Israeli army bombed one of Hamas' buildings, serving as its cyber base (Figure 68). While this attack partly affected the organization's cyber capabilities, Hamas has not stopped its cyber operations.



Figure 68 - One of the Hamas cyber command buildings destroyed by the IDF in 2019

- In 2020, Hamas-linked actors used cloud storage platforms (e.g., Dropbox, Google Drive) to disseminate spyware targeting Arab leaders. Lure content referenced high-profile figures such as Benjamin Netanyahu and Mohammed bin Salman.
- In 2021, the emergence of the "Gaza Hackers Team" and public claims from the Jerusalem Electronic Army revealed a broader ecosystem of pro-Hamas or affiliated cyber actors engaged in both psychological warfare and intelligence collection.

Advanced Phase (2022–2025): APT Behavior and Psychological Warfare

- In 2022, cybersecurity firm Cybereason reported a significant Hamas-linked campaign attributed to APT-C-23 (Arid Viper or Desert Falcons). This group employed advanced malware tools including: Barbie Downloader and BarbWire BackdoorVolatileVenom (trojanized messaging app). These tools demonstrated improved command and control (C2) protocols, evasion techniques, and user deception strategies. Later that year, Hamas officially revealed the existence of its cyber unit via propaganda videos, framing it as a central part of its resistance infrastructure (Figure 69). Additionally, the same year, Hamas officially revealed in a video that it had been operating a cyber unit for eight years with multiple cyberattacks against Israel (Figures 70 and 71)

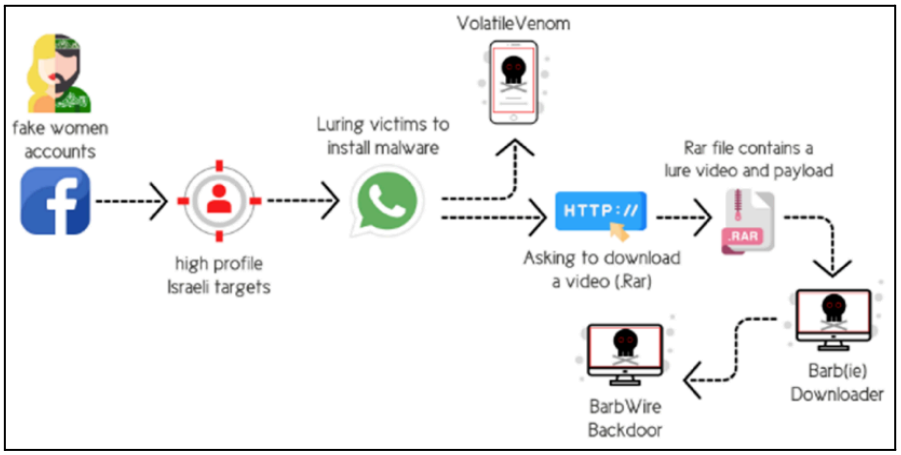


Figure 69 - Hamas Volatile Venom malware infection method (Source: Cybereason)



Figure 70 - A Hamas cyber fighter from their official Video



Figure 71 - Hamas' alleged cyber operations list

- In October 2023, the Hamas attack on Israel marked a turning point in hybrid warfare execution. While the world focused on the unprecedented scale of kinetic aggression, parallel cyber operations occurred, including:
    - Phishing and SMS-based disinformation campaigns targeting Israeli civilians (Figure 72).
    -



Figure 72 - Hamas fake SMS from Israeli Police

    - Defacements of Israeli news and municipal websites.Coordinated attacks on Israeli logistics and communications infrastructure.

- In 2024, Continued activity by Hamas-aligned APTs was detected, with updated variants of previous malware families and improved operational security, likely in response to enhanced Israeli cyber defenses and growing international scrutiny.

Proxy Groups and Cyber Affiliates

Hamas benefits from a decentralized network of sympathizers and proxy groups that expand its reach in cyberspace. Notable affiliates include:

- **Jerusalem Electronic Army**: Engaged in propaganda and defacement operations.
- **Gaza Hacker Team**: Frequently targeting Israeli networks and infrastructure.
- **Gaza Cybergang / Molerats**: Involved in espionage campaigns across the Middle East, often masquerading as legitimate NGOs or academic organizations.

Aditionally, since October 7, the terrorist organization has been able to rely on dozens of pro-Palestinian hacktivist groups.

Cyber-Enabled Financing: Cryptocurrencies and Anonymity

Cyber operations are intertwined with Hamas' innovative financing tactics. The organization has long utilized Bitcoin donation campaigns via its websites and Telegram channels, offering unique wallet addresses to donors to maintain anonymity. Messaging typically encourages contributions under the guise of supporting "resistance efforts" (Figures 73 and 74). However, the traceability of Bitcoin via blockchain analytics (e.g., Chainalysis, Elliptic) has pushed some groups, including Hamas, toward privacy coins such as Monero. This shift, observable since 2021, reflects an evolving financial strategy to obscure digital footprints and evade international sanctions. Cryptocurrency donations are typically laundered through:

Mixing services and wallet-hopping,

- Use of money mules to cash out,
- Integration into logistical operations such as equipment purchases or cyber tooling.

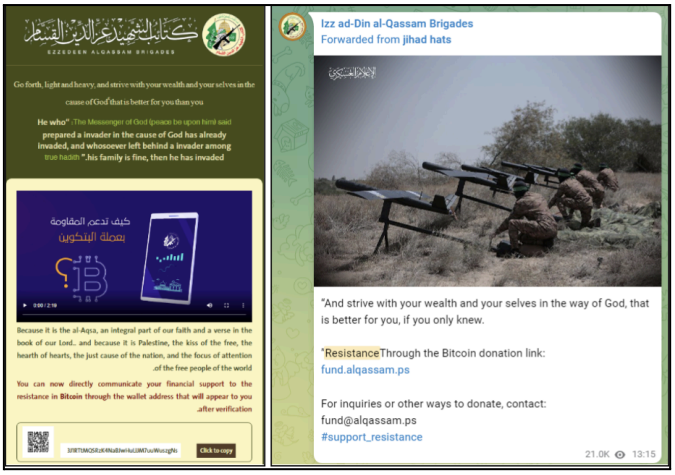


Figure 73 -Hamas urges financial support via Bitcoin or email on its website and Telegram.



Figure 74 – A Telegram post from the Jerusalem Electronic Army sharing a Bitcoin donation address (Source: Telegram).

Strategic Assessment

Until 2025, Hamas' cyber operations can be assessed as mid-level threats tactically competent, but still constrained by Gaza's infrastructural limitations and the group's technical ceiling. Their operations demonstrate:

- **Persistence**: Despite cyber losses (e.g., the 2019 Israeli airstrike on a Hamas cyber facility), operations resumed and evolved.
- **Adaptability**: Rapid adoption of new platforms and malware in response to countermeasures.
- **External Influence**: Hamas' cyber evolution appears correlated with increasing strategic ties to Iran, Turkey, and Qatar, which may provide covert technical or financial support.

By mid-2025, Hamas's cyber capabilities had been significantly weakened by extensive Israeli military operations in Gaza, which disrupted much of the group's internal infrastructure and personnel, including its cyber operatives.

Despite this, Hamas retains a limited cyber capability through external operatives and allied groups based outside Gaza, such as in Turkey, and with the apparent support of state actors such as Iran and Qatar. While its ability to launch sophisticated cyberattacks from Gaza has diminished, Hamas could continue to conduct cyber operations through phishing, malware, and information warfare campaigns, relying on collaboration with ideologically aligned hacktivist and cyber espionage groups abroad. Thus, although weakened, Hamas has not been eliminated as a cyber threat.

8.4.2 Hezbollah

Since the Second Lebanon War in 2006, Hezbollah has significantly expanded its cyber capabilities, transforming from a limited actor to a regional cyber threat. While the group and its affiliates have been active in cyberspace since the early 2000s, cyber operations have notably intensified in the last five years. These efforts serve Hezbollah's military and ideological objectives and are deeply integrated into its broader hybrid warfare strategy. With direct financial, technical, and strategic support from Iran, especially the Islamic Revolutionary Guard Corps' Quds Force, Hezbollah has become a cyber-enabled proxy actor, capable of espionage, sabotage, and influence operations across the Middle East and beyond. Hezbollah's cyber activities target Israel, the United States, GCC nations, Lebanese civil society, and occasionally European entities. The group uses cyberattacks to gather intelligence, shape public narratives, disrupt adversarial operations, and monitor domestic opponents. Cyber tactics include surveillance of smartphones and networks, penetration of telecom infrastructure, malware deployment, social engineering, and broad influence operations using fake profiles and digital propaganda.

Organizational Structure and Cyber Division

Hezbollah's cyber operations are managed under its intelligence wing, primarily by Technical Unit 1800 and Cyber Unit 121, with additional support and training provided by the IRGC's Quds Force. In recent years, a specialized cyber warfare unit was established, composed of seasoned hackers and cyber contractors jointly trained by Hezbollah and Iranian intelligence services. This cyber division is tasked with cyberattacks, espionage, and digital surveillance operations. Capabilities attributed to this unit include:

- Smartphone and Wi-Fi surveillance.
- Infiltration of government and corporate networks.
- Psychological operations and domestic political control.
- Advanced social engineering and phishing operations.
- Operations targeting cell phones, social networks, and infrastructure systems.

This unit's architecture supports strategic military objectives and internal dominance in Lebanon. Iran's support, from lessons learned post-Stuxnet (2010), includes technical training, malware development, and command and control infrastructure, allowing Iran to extend its cyber presence through Hezbollah beyond its borders.

Evolution of Cyber Capabilities (2006–2025)

Initial Phase (2006–2011): Early Propaganda and Communications Security

- 2006: During the Second Lebanon War, Hezbollah launched cyberattacks against Israeli-supporting states. These included website defacements and hijacking corporate communications and web hosting services in the U.S. to spread propaganda. Hezbollah began experimenting with secure communication systems, including encrypted radio networks for fighters, to avoid interception by foreign intelligence.

Surveillance and Social Engineering (2012–2016)

- 2013: Amid the Syrian Civil War, Hezbollah developed techniques to secure battlefield communications and deploy cyber tools for intelligence collection.

- 2015: Hezbollah-affiliated hackers under the alias "Lebanese Cedar" executed a global cyber espionage campaign targeting Israeli and Western organizations, especially those connected to defense and telecom sectors.

- The group transitioned from generic malware to tailored espionage tools designed to exfiltrate data and avoid detection.

Expansion and Regional Targeting (2017–2021)

- 2017: Hezbollah mimicked Hamas's tactics by using fake social media profiles (particularly of attractive women) to deliver spyware and malware to military and government targets.

- 2020: According to the *Daily Telegraph*, Hezbollah trained thousands of social media operatives to build digital "electronic armies" to manipulate online discourse across the Arab world.

- 2021: Cyber intelligence firm ClearSky revealed that Hezbollah's "Lebanese Cedar" APT had compromised over 250 servers in countries including Egypt, Israel, Jordan, the UK, and the US. Most targets were in the telecommunications sector, highlighting the group's emphasis on infrastructure intelligence collection (Figure 75).

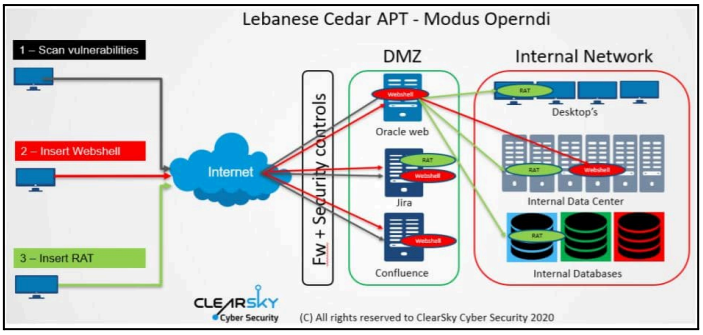


Figure 75 - Hezbollah Lebanese Cedar APT Modus Operandi (Source: ClearSky)

Advanced Phase (2022–2025): Regional Operations and Iranian Integration

From 2022 onward, Hezbollah became more deeply integrated into Iran's regional cyber ecosystem, cooperating with groups such as APT34 (OilRig) and APT35 (Charming Kitten). The group launched sophisticated attacks on Israeli infrastructure and broadened its espionage to include Gulf and European targets.

- 2022–2023 The group's cyber tools increasingly resembled those of Iranian APTs, including multi-stage backdoors, credential theft frameworks, and ICS-reconnaissance malware.
- In 2023, the operation dubbed "Cedar Rain" targeted Israeli logistics, water treatment facilities, and border infrastructure, including attempts to interfere with Iron Dome radar and command software. These attacks were coordinated with missile and drone activity, illustrating Hezbollah's hybrid warfare model. Hezbollah also deployed spyware against domestic rivals in Lebanon, including opposition politicians and journalists. Investigations revealed targeting of Kataeb Party members and civil society activists using spyware with functionality similar to Iranian-designed implants. Following Hamas's October 7 assault on Israel, Hezbollah ramped up coordinated cyber efforts as part of a broader regional campaign. Activities included:
    - Cyber intrusions into Israel northern command centers.
    - Propaganda dissemination through fake videos and audio deepfakes on social platforms.
    - An attempted infiltration of the Israeli Ministry of Health to create panic by spreading disinformation on water contamination.
    - Simultaneous kinetic and cyber operations aimed at overwhelming Israel's early warning and emergency response systems.

These efforts show the group's increasing use of synchronized digital and physical attacks in coordination with other Iran-aligned groups.

Proxy Groups and Cyber Affiliates

Hezbollah's cyber footprint is amplified by a network of affiliated or covert cyber groups, including:

- **Lebanese Cedar APT / Volatile Cedar**: Primary espionage unit responsible for dozens of intrusions globally.
- **Al-Quds Electronic Army**: Focuses on psychological warfare and social media manipulation.
- **Green Leakers**: Anonymous pro-Hezbollah actor leaking sensitive data and targeting Israeli infrastructure.
- **Iranian IRGC and MOIS Cyber Units**: Hezbollah acts as both beneficiary and operational partner of Iranian APT groups.

These actors operate in parallel or in support of Hezbollah's core cyber objectives and occasionally overlap in tooling and infrastructure.

Cyber-Enabled Financing: Crypto and Iranian Support

Hezbollah has increasingly turned to cryptocurrency as a tool to bypass international sanctions and secure funding for its activities. In the face of tightened global financial regulations and enhanced scrutiny of traditional banking channels, the group has leveraged digital currencies to anonymize transactions and obscure financial trails. This strategic use of crypto assets not only aids in sustaining its operational capabilities but also facilitates the financing of cyber operations and the procurement of technological infrastructure. Methods include:

- Accepting donations in Bitcoin, Monero, and Tether (USDT) via Telegram and anonymous forums.
- Utilizing wallet-hopping, mixing services, and decentralized exchanges (DEXs) to obscure the flow of funds.
  Integrating crypto into operational expenses, including:
    - VPNs and proxy infrastructure.
    - C2 servers hosted in foreign jurisdictions.
      Licensing and procurement of malware or zero-day exploits via darknet markets.

In addition to soliciting donations often through seemingly legitimate charitable fronts Hezbollah has also turned to cryptocurrency mining as a revenue stream.

The group has established Bitcoin mining farms (Figure 76), particularly in areas where they exert territorial control, to generate funds in a manner that is difficult to trace and largely outside the reach of traditional financial oversight. This diversification of funding sources not only shields the organization's leadership from direct financial exposure but also reinforces its ability to operate independently of conventional banking systems and sanctions.



Figure 76 - Hezbollah Cryptocurrency mining equipment

Strategic Assessment

As of 2025, Hezbollah’s cyber capabilities have been significantly degraded following a sustained Israeli campaign involving cyber operations, electronic warfare, and targeted kinetic strikes. These actions have dismantled portions of Hezbollah’s cyber infrastructure, eliminated or incapacitated key personnel, and forced the group into a reactive and fragmented operational posture.

Previously considered a mid-tier cyber actor with regional offensive reach, Hezbollah depends on Iranian support for technical expertise, infrastructure, and strategic direction. Its independent cyber operations have been reduced to low-level disinformation campaigns, social engineering attempts, and internal communication efforts, with little evidence of complex or high-impact activity in the first half of 2025.

Israeli intelligence and cyber units, most notably Unit 8200, have succeeded in disrupting command-and-control nodes, degrading Hezbollah’s surveillance capabilities, and exposing digital assets linked to both operational and propaganda functions. This has left Hezbollah struggling to rebuild while under persistent surveillance and pressure. While Hezbollah retains latent potential through its integration with Iran’s cyber doctrine, the group’s role has shifted from that of an independent cyber actor to a proxy vector for low-intensity influence operations. Tehran appears increasingly cautious, keeping core cyber assets under tighter control. Hezbollah remains a diminished but not defunct cyber threat.

Its future capabilities will depend on the Iranian willingness to reinvest and on the group's ability to recruit and train new cyber operatives. For now, Hezbollah's strategic focus in cyberspace is defensive, mainly limited, and subordinate to broader Iranian cyber agendas.

8.4.3 Islamic State (ISIS/ISIL)

Since its rapid territorial rise in 2014, the Islamic State (IS) has evolved from a jihadist insurgency into a digitally native terrorist entity with a robust cyber-enabled warfare doctrine. While IS lacks the technical depth of state-sponsored actors like Hezbollah or Iran's APTs, it has developed a unique model that fuses cyber innovation with propaganda, asymmetric warfare, and decentralized operations. Unlike Hezbollah, which operates within a state-aligned structure, IS has embraced a fluid, transnational cyber strategy reliant on ideologically motivated volunteers, dark web networks, and encrypted communication tools.

IS's cyber activities prioritize influence, recruitment, psychological warfare, and counter-surveillance rather than advanced cyber-espionage. Nonetheless, its experimentation with hacking, cryptocurrencies, and secure communication channels has made it a persistent cyber threat, especially in Europe, South Asia, and parts of Africa. The group also leverages open-source tools, digital obfuscation techniques, and darknet infrastructure to maintain operational continuity despite territorial losses.

Organizational Structure and Digital Units

IS's cyber operations have been decentralized by design, functioning more like a swarm of ideologically aligned actors than a formalized state apparatus. Key components include:

- **Diwan al-Hisbah (Morality Police Cyber Unit)**: Enforced digital shariah law during the caliphate era and engaged in online censorship, surveillance, and enforcement of IS propaganda standards.
- **Electronic Horizon Foundation**: A now-dismantled cyber training and security awareness entity that provided online tutorials to IS supporters on secure communications, anti-surveillance tactics, and cyber hygiene.
- **United Cyber Caliphate (UCC)**: A loose coalition of IS-affiliated cyber cells that claimed responsibility for several low-grade cyberattacks and hacking operations, often targeting Western institutions and media outlets.
- **Dark web and Telegram-based cells**: Dispersed nodes used for propaganda dissemination, recruitment, fundraising, and operational command via encrypted channels.

IS's digital structure emphasizes:

- **Secure communications** (e.g., Signal, Telegram, Tails OS).
- **Low-skill hacking tutorials** to democratize cyber violence.
- **Propaganda and media warfare** via Al-Hayat Media Center, Amaq News Agency, and decentralized social media "reshares".

Evolution of Cyber Capabilities (2014–2025)

Early Phase (2014–2016): Cyber Jihad and Media Dominance

- In 2014 IS declared its caliphate, it launched a massive media campaign across Twitter, YouTube, and Facebook. Cyber efforts focused on:
    - Dissemination of high-production-value videos.
    - Live tweeting of battlefield victories and executions.
    - Hijacking hashtags (#WorldCup, #Ebola) to amplify reach.

- In 2015, IS sympathizers, under the "Cyber Caliphate" label, hacked the Twitter and YouTube accounts of the U.S. Central Command. Although technically unsophisticated, the event had high propaganda value and revealed the group's strategic grasp of information warfare. Moreover, the terrorist group even released a list of applications with a ranking of recommended private messaging. ISIS considered Telegram a secure and reliable communication application, and they encouraged their supporters to use Telegram to discuss sensitive issues such as travel to Islamic State-controlled territory. The Islamic State has also created multiple public channels on Telegram to deliver news updates and propaganda messages through its news agency, Amaq Agency. On the defensive side, the Islamic State published a manual in 2015 on how to avoid intelligence surveillance and what to do to stay safe and anonymous online. Furthermore, the Electronic Horizon foundation Afaq, established in 2016 and aligned with the ideology of ISIS, published a magazine a few years later to raise awareness among ISIS supporters and media activists about operational security (Figure 78).



Figure 78 - Magazine from Afaq, which aims at raising security awareness among ISIS supporters (source: JihadoScope)

Middle Phase (2017–2020): Digital Decentralization and Counter-Surveillance

- In 2017, following the fall of Raqqa, IS adopted a more decentralized cyber strategy. Encrypted channels became the norm, and IS issued detailed guides (via Electronic Horizon) on avoiding Western intelligence interception.
    - Expanded use of VPNs, encrypted messengers, and OPSEC tutorials.
    - Released manuals for remote lone-wolf attacks and cyber sabotage using off-the-shelf tools.
- In 2019, IS-linked hackers defaced hundreds of websites across Southeast Asia, the Balkans, and Latin America, replacing pages with IS logos and messages. These low-level operations sought symbolic dominance rather than strategic impact.

Advanced Phase (2021–2025): Cyber Persistence and Newfronts

- 2021–2022: IS resumed cyber propaganda in Africa and South Asia, focusing on Nigeria (ISWAP), Mozambique, and Afghanistan (IS-Khorasan). Operations included: Social media botnets amplifying executions and attacks, online training cells for tech-savvy recruits in Pakistan and Indonesia.
    - In 2021, the Islamic State released a video to encourage hacking and, at the same time, to try to recruit hackers, but without any official group name. These calls to recruit hackers did not have the expected effect or results.
    - However, as of 2022, the organization still has multiple supporters active on several Telegram channels or underground websites, promoting the Islamic State ideology, and discuss the organization's activities (Figures79).



Figure 79 - Some ISIS Telegram channels still active in 2022

- In February, the Islamic State posted a guide called "Drone Survival Guide" on RocketChat, which provided technical information on different types of drones and tips for defending against them (Figures 79 and 80)

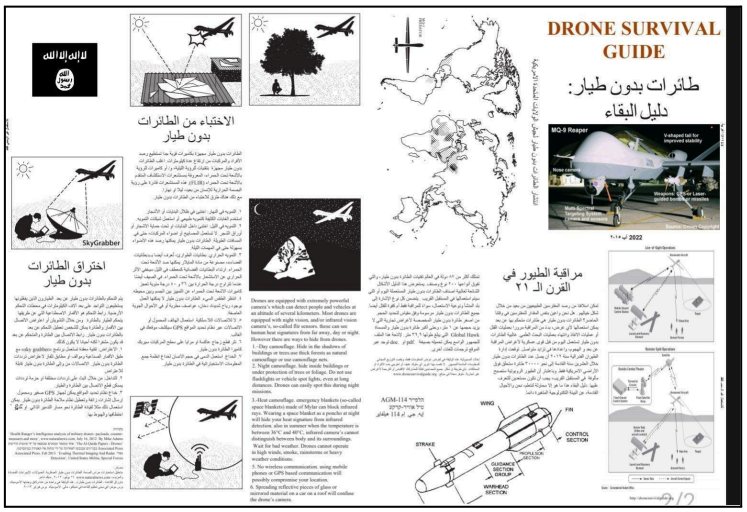


Figure 79 - A survival guide created by the IS group teaches how to protect against drones on RocketChat (Source: dark web)

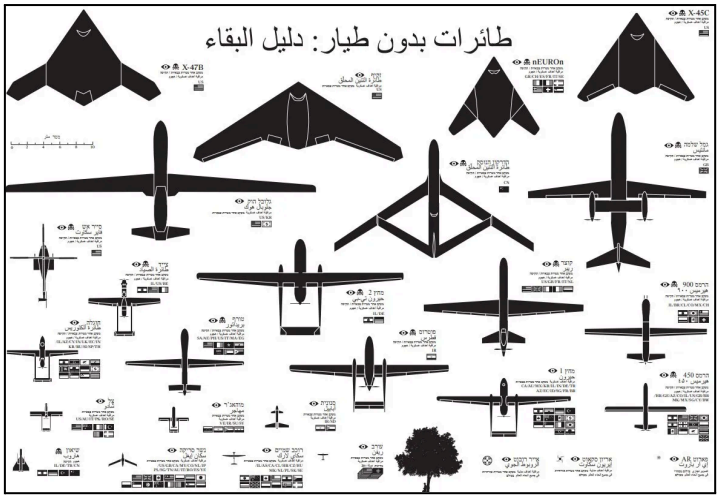


Figure 80 - A survival guide created by the ISIS group teaches how to protect against drones on RocketChat (Source: dark web)

- **In 2023,** the U.S. intelligence identified IS-Khorasan cyber cells in Kabul disseminating operational manuals via .onion forums and running pro-IS channels on blockchain-based decentralized networks. Analysts noted IS experiments with:
    - Web3-based social platforms to bypass moderation.
    - Cryptocurrency-based bounty systems for identifying Western targets.

- **2024–2025** IS cyber propaganda resurged via AI-manipulated media:
    - Deepfake videos of beheadings are designed to confuse attribution and inflate IS's image.
    - Voice-cloned propaganda messages from deceased leaders like Abu Bakr al-Baghdadi to sustain ideological continuity.

Proxy Groups and Sympathetic Cells

Although IS does not maintain a traditional network of proxies like Hezbollah, it benefits from:

- Lone-wolf hackers and digital sympathizers who act on IS's behalf.
- Regional affiliates (e.g., IS-K, ISWAP, IS-Mozambique) who develop localized cyber infrastructures.
- Pro-IS media cells (e.g., Nashir News, Halummu Foundation) that distribute multilingual propaganda and training guides.

These actors function with high autonomy, often without direct IS command, but remain ideologically consistent and strategically aligned.

Cyber-Enabled Financing: Crypto, Crowdfunding, and Obfuscation

IS was among the earliest terrorist groups to adopt cryptocurrency for financing, especially after 2017. Though not as technically sophisticated as Hezbollah's crypto apparatus, IS has used:

- Bitcoin, Monero, and Dash for anonymous donations.
- Darknet crowdfunding through forum-based "zakat" platforms.
- QR code-based donation drives in propaganda videos and encrypted chat groups.

Documented methods include:

- Use of mixers and tumblers to obscure transaction trails.
  Wallet-hopping strategies to evade tracking.
- One-time-use wallets generated per donor to maximize anonymity.

IS has also experimented with:

- NFTs for laundering money and embedding propaganda.
- DeFi platforms to transfer value across borders without centralized oversight.

These efforts are often fragmented and amateurish, but ongoing adaptation and innovation suggest a willingness to explore emerging technologies for illicit finance.

Strategic Assessment

As of 2025, the Islamic State's cyber threat persists primarily through ideological diffusion and digital resilience. While it lacks the advanced technical capabilities of state-supported actors, IS remains dangerous due to:

- It's the ability to radicalize and mobilize through digital propaganda.
  It's a flexible, adaptive use of secure technologies and decentralized platforms.
  It's an embrace of symbolic cyber operations to amplify psychological impact.

Western intelligence efforts have significantly disrupted centralized IS media units, including the takedown of the Electronic Horizon Foundation and seizure of hundreds of IS-linked Telegram accounts. However, the group's digital decentralization and persistent ideological magnetism continue attracting global sympathizers. IS's future cyber trajectory will likely include:

- Greater use of AI-generated content for propaganda.
- Integration of emerging technologies like decentralized social media, smart contracts for fundraising, and quantum-resistant encryption tools.

- Persistent targeting of weak digital infrastructures in unstable regions, particularly in Africa and Southeast Asia.

Although IS is not a high-tier cyber actor, its blend of ideological zeal, digital adaptability, and decentralized resilience ensures it remains a threat across physical and virtual battlefields.

8.4.4 Al-Qaeda

Al-Qaeda, one of the most notorious terrorist organizations of the 21st century, has long served as a global symbol and architect of transnational jihadist ideology. Its hallmark attack, the September 11, 2001 terrorist strikes on the United States, demonstrated how a non-state actor with limited resources could orchestrate large-scale operations with vast strategic and psychological consequences. Since then, Al-Qaeda has evolved across multiple domains, including cyberspace, where it has sought to maintain ideological relevance and operational continuity in the face of leadership losses and battlefield setbacks. While Al-Qaeda never embraced digital warfare with the same intensity or innovation as the Islamic State, it has played a foundational role in shaping jihadist cyber culture. Since the late 1990s, the group has leveraged cyberspace for ideological dissemination, recruitment, strategic communication, and, to a lesser extent, operational security. It has inspired and cultivated the broader concept of “cyber jihad,” enabling a new wave of Islamist digital activism across forums, encrypted messaging platforms, and dark web communities.

Unlike groups with more aggressive cyber operations like Hamas or Hezbollah, Al-Qaeda’s digital doctrine has remained predominantly focused on propaganda, ideological transmission, and secure communication rather than on offensive cyberattacks. Nonetheless, the group's enduring ideological magnetism and strategic patience continue to make it a significant player in the evolving landscape of cyber-enabled terrorism.

Organizational Structure and Digital Arms

Al-Qaeda’s cyber apparatus is less centralized and technologically capable than other groups, but several entities have played a role in its digital engagement:

- **Al-Fajr Technical Committee**: Established in the early 2000s, Al-Fajr developed the group’s first encryption tools and digital security protocols. In 2013, it released its own proprietary encryption software to facilitate secure intra-network communications (Figure 29).

- **Al-Qaeda Electronic Army**: Announced in 2015, this offshoot focused on low-level cyberattacks such as website defacements and occasional DDoS campaigns (Figure 28). It lacks the operational sophistication of state-aligned APTs or even pro-IS cyber cells.
- **Jaish al-Malahem al-Electronic**: A pro-Al-Qaeda media and tech entity active since the late 2010s. In 2020, it released a digital magazine on Telegram with guidance on cybersecurity, operational tactics, and ideological materials (Figure 30). 2021 it issued recruitment calls for media specialists and hackers (Figure 31).

These units collectively form the backbone of Al-Qaeda's cyber-enabled capabilities, though they remain fragmented and primarily focused on information operations rather than direct cyber warfare.

Evolution of Cyber Capabilities (1998–2025)

Early Phase (1998–2010): Ideological Pioneering in Cyberspace

Al-Qaeda was an early adopter of digital tools for ideological propagation:

- Created websites and web forums to distribute statements, videos, and ideological texts.
- Released "as-Sahab" media productions via password-protected forums.
- Developed early OPSEC practices using rudimentary encryption and anonymous remailers.

  This phase laid the groundwork for global cyber jihad and influenced other jihadist groups' digital behavior.

Middle Phase (2011–2018): Decentralization and Digital Survival

Following the death of Osama bin Laden in 2011 and the rise of the Islamic State, Al-Qaeda adopted a more cautious and decentralized cyber strategy:

- Use of encrypted email chains and private forums for communication.
- Transition to commercial encrypted platforms like Telegram, Threema, and Signal.
- Focused on publishing ideological content from affiliates such as AQAP and al-Shabaab.

  While rivaled in visibility by ISIS during this time, Al-Qaeda preserved its digital base through tight-knit media networks and selective digital releases.

- In 2013, according to deep research by the company Recorded Future , the Al-Fajr Technical Committee, a mainstream Al-Qaeda organization, created an encryption software program (Figure 81)

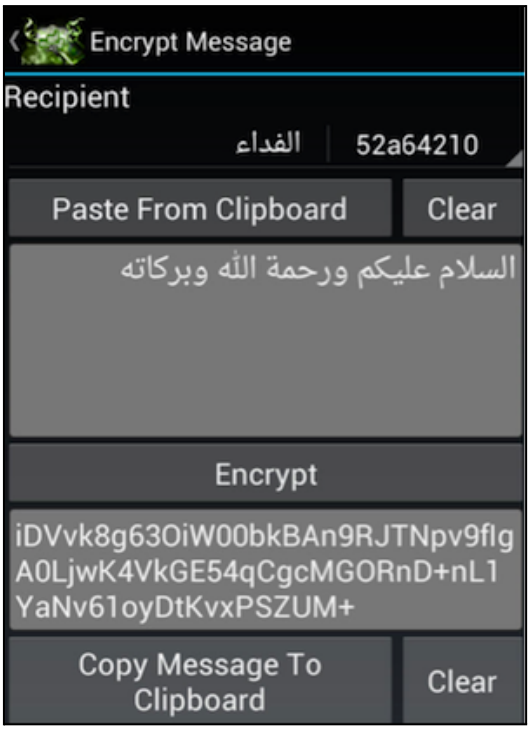


Figure 81 – Encrypted messaging software developed by Al-Fajr (Source: Recorded Future)

- In 2015, Al-Qaeda Electronic announced its formation as a new branch of Al-Qaeda to be engaged in cyber warfare (Figure 82). However, the organization has never been involved in severe or successful cyberattacks. Most cyberattacks launched by the Al-Qaeda Electronic branch have consisted of website defacements against relatively low-value targets. The group has also occasionally launched DDoS attacks.



Figure 82 - Symbol of the Al-Qaeda Electronic Army

Advanced Phase (2019–2025): Resilience and Low-Tech Persistence

- In 2020, an Al-Qaeda supporter group, Jaish al-Malahem al-Electronic, posted a magazine on Telegram with advice on various topics, from online safety to carrying out attacks (Figure 83).



Figure 83 – A magazine with different advices, from online safety to carrying out different attacks on Telegram

As of 2025, Al-Qaeda's cyber strategy continues to revolve around ideological transmission, community building, and decentralized security:

- Encrypted Communications: Continued use of Telegram, Rocket.Chat, and custom OPSEC tools.
- Cybersecurity Awareness: Jaish al-Malahem materials promote safe browsing, VPNs, metadata scrubbing, and anonymous communication practices.
- Media Propagation: Revival of As-Sahab productions with multilingual subtitles and cross-platform publication to reach global audiences.

Despite minor forays into cyberattacks (mostly symbolic website defacements), Al-Qaeda has avoided complex offensive operations. The group instead emphasizes psychological and ideological warfare, avoiding high-risk digital engagements that could expose its leadership or network.

Proxy Groups and Affiliated Media Cells

Al-Qaeda's networked structure allows its ideology to be channeled through multiple affiliated and semi-autonomous groups:

- AQAP (Al-Qaeda in the Arabian Peninsula): Maintains a digital media presence and OPSEC culture similar to core Al-Qaeda.
- Al-Shabaab (Somalia) and AQIM (North Africa): Produce propaganda videos, issue communiques via encrypted channels, and occasionally contribute to digital jihad materials.
- Media wings such as As-Sahab, Global Islamic Media Front (GIMF), and al-Malahim Media continue to shape the visual and narrative elements of Al-Qaeda's message.

These groups also serve as conduits for cybersecurity materials, digital strategy discussions, and ideological reinforcement, forming an **ecosystem of decentralized media jihad**.

Cyber-Enabled Financing and Anonymity Tools

While not as active as IS in crypto-finance, Al-Qaeda has experimented with anonymous funding models:

- Bitcoin and Monero donation campaigns advertised in PDF leaflets and Telegram channels.
- Use of dark web forums for financial discussions and potential "zakat" campaigns.
- Supporters reportedly use one-time wallets and mixers, though with less frequency and sophistication than IS.

Recent intelligence reports suggest limited but ongoing interest in privacy-preserving technologies, especially in regions with high financial surveillance.

Strategic Assessment

As of 2025, Al-Qaeda's cyber threat level remains moderate to low, with key features including:

- Strategic restraint in launching offensive cyberattacks.
- Persistence in ideological messaging, often via encrypted and decentralized networks.
- Cultural influence on global jihadist cyber culture, even as IS dominates propaganda.

Al-Qaeda's cyber arm remains underdeveloped, constrained by technological limitations, aging leadership, and a strategic preference for physical over digital disruption. However, the group's resilience in information warfare and OPSEC practices ensures that it continues to inspire and mobilize.

Future trajectories may include:

- Increased collaboration with cyber-capable affiliates such as AQAP.
- Use of AI-assisted propaganda tools to modernize outreach.
- Adoption of Web3-based tools to enhance anonymity and coordination.

8.5 Hacktivism

Hacktivism has evolved into a multifaceted phenomenon characterized by various campaigns and collective actors, each utilizing distinct digital tactics to advance ideological, political, or social causes. The group Anonymous, arguably the most well-known hacktivist collective, is central to this movement, which has become emblematic of decentralized, leaderless activism in cyberspace. Anonymous gained widespread attention through its early campaign,s such as Operation Payback (2010), which launched coordinated DDoS attacks against entities perceived to suppress internet freedom, including financial institutions and organizations opposed to WikiLeaks. Later, Anonymous engaged in Operation Tunisia and Operation Egypt, supporting the Arab Spring uprisings by targeting government websites and enabling communication channels, thereby amplifying calls for democracy and human rights in authoritarian regimes. Beyond Anonymous, groups such as LulzSec have emerged, blending hacktivism with a more chaotic and often provocative approach, focusing on exposing security weaknesses and embarrassing targets ranging from law enforcement agencies to media conglomerates. Other hacktivist organizations and campaigns have focused on specific issues, such as WikiLeaks, which while not strictly a hacktivist group, has collaborated with hacker communities to release classified documents revealing government and corporate misconduct. The Syrian Electronic Army, a pro-government hacking group, has engaged in cyber operations that blur the lines between hacktivism and cyberwarfare, illustrating how digital activism can be co-opted or aligned with state interests. These campaigns often employ a combination of website defacements, information leaks, social engineering, and DDoS attacks to disrupt operations, expose perceived corruption, or sway public opinion.

The impact of these hacktivist campaigns is profound, as they have demonstrated the power of cyber tools to challenge entrenched power structures, influence social movements, and expose systemic abuses. However, they have also highlighted the security vulnerabilities of critical infrastructure and the difficulties governments face in attribution and enforcement, given the anonymous and transnational nature of hacktivist networks.

The decentralized structure of groups like Anonymous complicates traditional law enforcement responses, while their symbolic actions inspire both solidarity and controversy within civil society and the cybersecurity community alike. Ultimately, the diverse range of hacktivism campaigns underscores the fluid boundary between activism and cyber conflict, raising ongoing debates about the legitimacy, ethics, and consequences of employing hacking as a form of protest and political engagement in the digital age.

8.5.1 Prominent Hacktivist Groups

In the evolving landscape of digital activism and cyber warfare, hacktivist groups have emerged as potent non-state actors leveraging cyberspace to promote ideological, political, and nationalistic agendas. These groups, often decentralized and transnational, vary widely in motivations, tactics, and targets. For instance, NoName057(16), a Russian-based collective, is known for orchestrating widespread DDoS campaigns against Ukraine, NATO allies, and Israel, often aligning with pro-Kremlin entities such as the Cyber Army of Russia Reborn. In contrast, Guacamaya, rooted in Latin America, exposes environmental and anti-imperialist grievances through large-scale data leaks, such as the revelatory "NarcoFiles." Similarly, the Belarusian Cyber Partisans have taken a militant stance against their authoritarian regime, disrupting critical infrastructure and leaking intelligence data. On the other side of the political spectrum, the Indian Cyber Force (ICF) channels nationalist fervor into anti-Pakistan cyber offensives. At the same time, groups like RipperSec (Malaysia), Sylhet Gang (Bangladesh), and Spider-X (Indonesia) engage in digital resistance aligned with the Palestinian cause, primarily targeting U.S. and Israeli systems.

Meanwhile, Dark Storm Team combines pro-Palestinian and anti-Israel sentiments with cybercrime tactics like ransomware. Finally, Keymous+, whose origins remain murky, is characterized by its pro-Russian and anti-Western DDoS activity focused on Eastern Europe.

Together, these groups demonstrate how digital platforms have become both battleground and amplifier for ideological warfare, blurring lines between hacktivism, state influence, and cybercrime. The following list (non-exhaustive) is a brief overview of several prominent hacktivist groups, each with distinct political motivations, ideological alignments, and cyber capabilities.

NoName057(16)

- **Origin**: Russia
- **Focus**: Anti-Western, pro-Russian agenda
  Tactics: Large-scale DDoS attacks using the DDoSia tool
- **Targets**: Ukraine, NATO countries, Israel

- **Affiliations**: Collaborates with groups like Cyber Army of Russia Reborn and Z-Pentes

Dark Storm Team

- **Origin**: Pro-Palestinian, with members in Morocco
- **Focus**: Anti-Israel campaigns
  Tactics: DDoS attacks, ransomware
  Notable Attacks: March 2025 DDoS attack on X (formerly Twitter)

Indian Cyber Force (ICF)

- **Origin**: India
  Focus: Pro-India, anti-Pakistan and anti-Muslim sentiment
- **Tactics**: DDoS attacks, data breaches
- **Notable Attacks**: Breached Pakistan's IRIS portal and Habib Bank's employee systems

Guacamaya

- **Origin**: Latin America (Chile, Colombia, Mexico, Peru)
  Focus: Anti-imperialism, environmentalism
- **Tactics**: Data leaks, exposing corporate and government corruption
- **Notable Leaks**: NarcoFiles, revealing global drug trade details

Cyber Partisans

- **Origin**: Belarus
  Focus: Opposition to Belarusian government and Russian influence
  Tactics: Railway disruptions, data leaks
  Notable Attacks: Infiltrated Belarusian KGB network, leaked over 8,600 agent identity

RipperSec

- **Origin**: Malaysia
- **Focus**: Pro-Palestinian activism
- **Tactics**: DDoS attacks using MegaMedusa tool
- **Targets**: U.S.-based organizations

Sylhet Gang (SG)

- **Origin**: Bangladesh
  Focus: Anti-India, pro-Palestinian sentiment
- **Tactics**: DDoS attacks
- **Notable Attacks**: Targeted U.S. government and healthcare systems

Spider-X

- **Origin**: Indonesia
- **Focus**: Opposition to U.S. foreign policy, support for Palestinian cause
- **Tactics**: DDoS attacks
- **Notable Attacks**: Targeted U.S. media outlets like CNBC and CN

Keymous+

- **Origin**: Unclear, possibly Eastern Europe
- **Focus**: Pro-Russian, anti-Western agenda
- **Tactics**: DDoS attacks
- **Notable Attacks**: Targeted Baltic and Eastern European digital assets

Many hacktivist groups actively collaborate with one another to execute coordinated offensive operations (Figure 84). These alliances are often driven by shared ideologies, mutual strategic interests, or complementary technical skills. By pooling resources and expertise, these groups increase the effectiveness and reach of their campaigns, whether they aim to disrupt critical infrastructure, expose sensitive information, or make political statements. Such collaborations can be temporary and goal-specific or evolve into long-term partnerships, reflecting a growing trend of collective action in the hacktivist landscape.

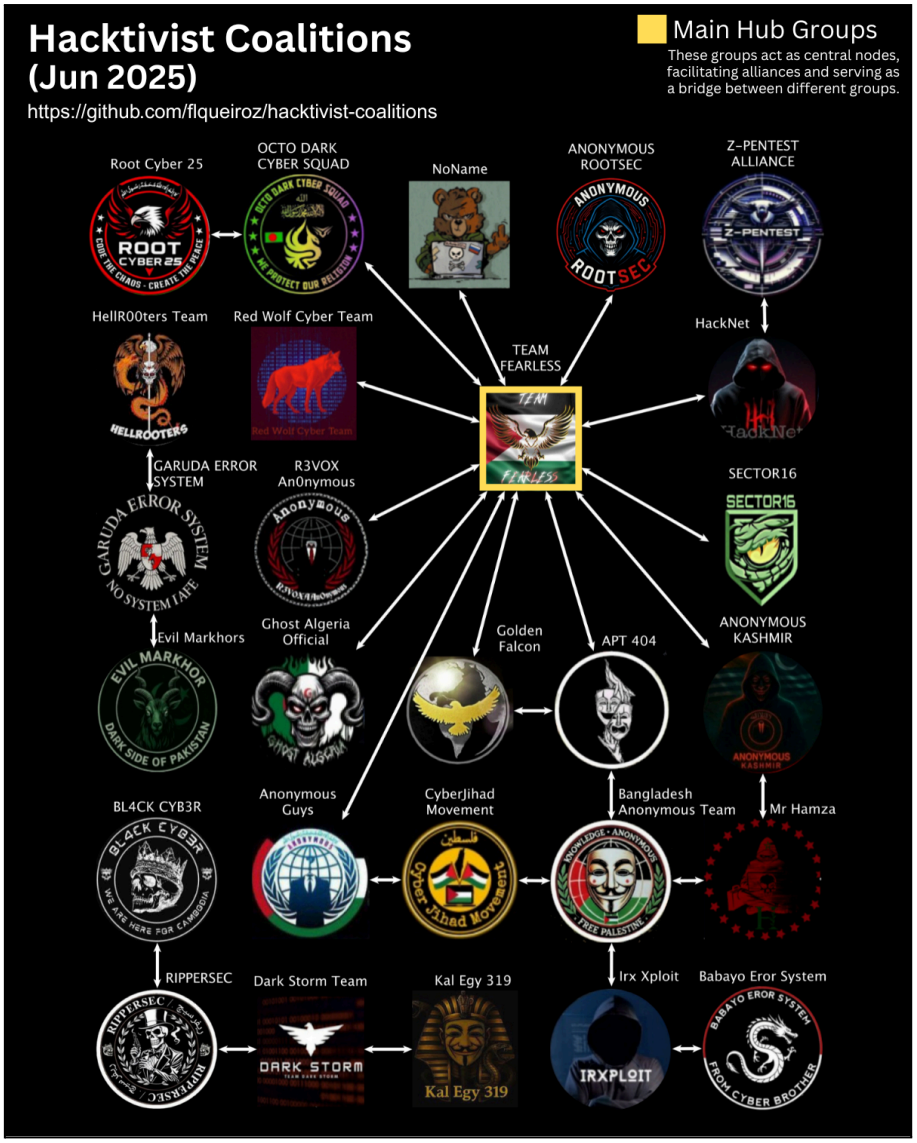


Figure 84 - Hacktivist coalitions as of June 2025 (Source: Github/flqueiroz)

8.5.2 Cooperation Between Hacktivists and Cybercriminals

In recent years, cybersecurity analysts have observed an increasing convergence between ideologically driven hacktivist groups and cybercriminal or politically motivated hacking collectives. Although their foundational ideologies may differ, these groups have found common ground in shared adversaries and tactical objectives. One notable example of this collaboration is the growing operational alliance between the Islamist-aligned hacktivist group *Anonymous Sudan* and the pro-Russian collective *KillNet*.

Anonymous Sudan

Anonymous Sudan emerged in early 2023, initially claiming to defend Sudan's sovereignty and national interests. However, its operations quickly evolved to target foreign entities perceived as hostile to Islam. The group has since carried out cyberattacks against countries such as Sweden, Denmark, France, the United States, and, most recently, India, citing religious and cultural grievances.

The group is primarily known for:

- **Distributed Denial of Service (DDoS) attacks.**
- **Website defacements.**
- **Data breaches**.

In mid-2024, Anonymous Sudan claimed responsibility for cyberattacks on French hospitals and government websites, including an alleged breach of the national airline, Air France (Figure 85). These incidents prompted formal investigations by French intelligence and judicial authorities. The group remains highly active on Telegram, announcing upcoming operations, sharing results, and amplifying its ideological messaging. Notably, it recently claimed cyberattacks on Indian hospitals, citing perceived anti-Muslim policies as justification (Figure 86). Despite the group's branding as "Sudanese," researchers have raised questions about its origins and affiliations, with some analysts suggesting the group may not be based in Sudan at all, but instead serve as a proxy for broader geopolitical agendas.

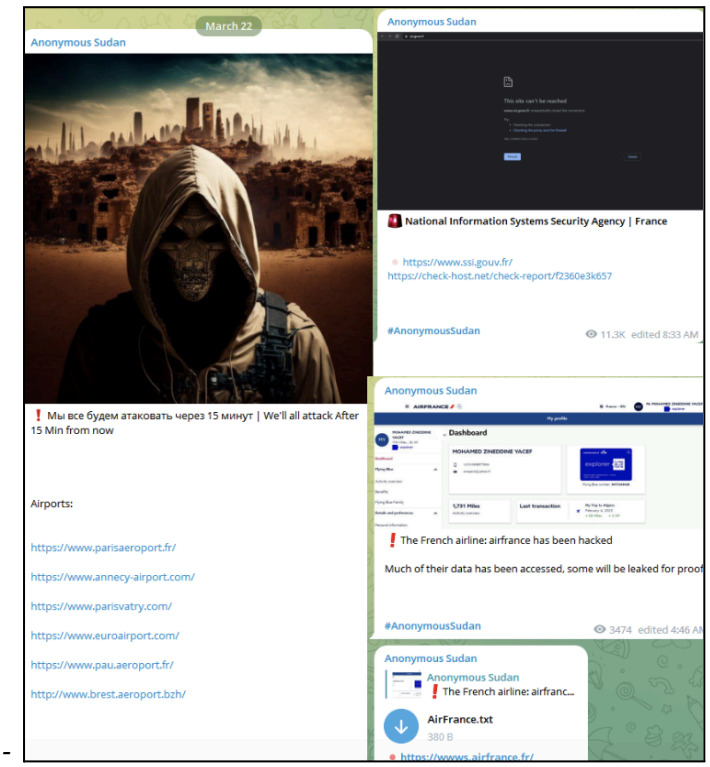


Figure 85 - Anonymous Sudan operation messages on Telegram



Figure 86 - Anonymous Sudan claiming on Telegram to target Indian hospitals

KillNet

KillNet surfaced in early 2022 and has become one of the most prominent pro-Russian cyber groups operating in the context of the Russia–Ukraine conflict. Initially known as a DDoS-for-hire service, KillNet has since rebranded itself as a patriotic group defending Russian interests in cyberspace. The group has primarily engaged in:

- **DDoS attacks** on critical infrastructure in NATO countries,
- **Disruption of government and media websites**, and
  Information operations leveraging Telegram and other social platforms.

KillNet does not appear to employ highly sophisticated tactics like advanced persistent threat (APT) actors or engage in ransomware extortion. Nonetheless, its attacks have temporarily disabled services across Europe and North America, including airport systems, healthcare services, and military-affiliated institutions. Although KillNet claims no formal ties to the Russian state, its operations frequently align with Russian geopolitical objectives (Figure 87). In 2024, the group claimed responsibility for cyberattacks that allegedly disrupted up to 40% of NATO's electronic infrastructure. It also published credentials and login data allegedly exfiltrated from NATO School Oberammergau (NSO), including sensitive email and password information (Figure 88).



Figure 87 - Announcement of Anonymous Sudan being a member of KillNet on Telegram

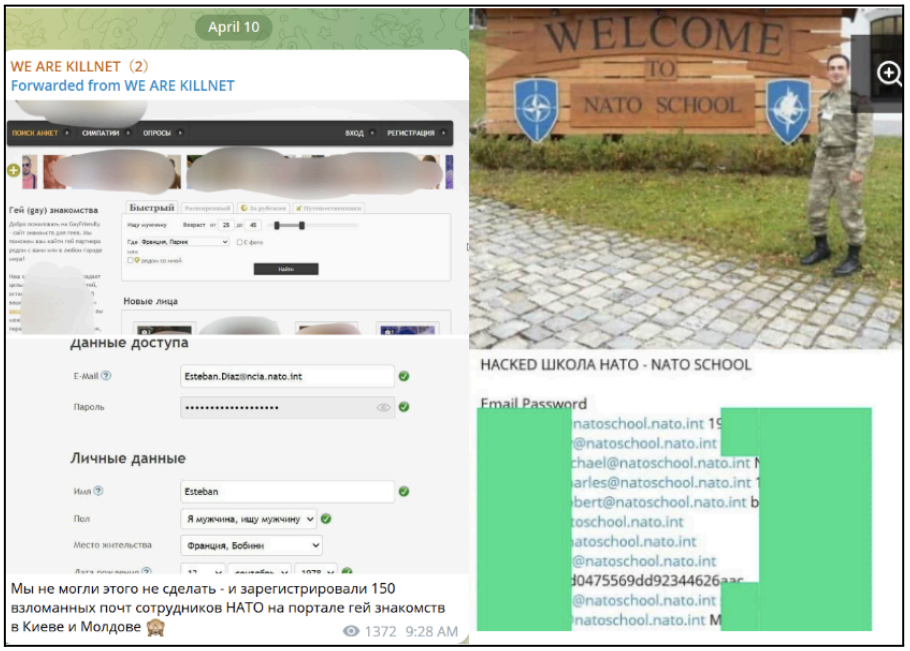


Figure 88 - On the left, KillNet logged alleged stolen NATO credentials on gay dating sites. On the right are stolen credentials (email and passwords)

Part III: Cyber Geopolitics and Alliances

Chapter 9: Cyber Diplomacy in a Multipolar World

In a multipolar world, cyber diplomacy must address a fragmented international system where states pursue differing and often competing visions of digital governance. The absence of universally accepted cyber norms complicates deterrence doctrines, as attribution in cyberspace remains ambiguous and enforcement mechanisms are weak. While the United Nations has made incremental progress through the Open-ended Working Group (OEWG) and the Group of Governmental Experts (GGE), substantial gaps remain between Western liberal democracies advocating for an open and secure internet and authoritarian regimes favoring sovereign control over cyberspace. Deterrence doctrines, especially those modeled after Cold War strategies, struggle to find traction in cyber realms where retaliation may be covert, delayed, or asymmetric, challenging traditional notions of proportional response and strategic stability.

Challenges in establishing global rules: Crafting global cyber rules faces significant barriers, including geopolitical rivalry, lack of trust, and differing legal traditions. The decentralized and borderless nature of the internet clashes with the state-centric frameworks of international law. Key players like the U.S., China, and Russia advocate for divergent governance models, undermining the consensus necessary for robust treaties. Moreover, the rapid evolution of technology outpaces diplomatic processes, leaving frameworks obsolete before they are widely adopted. Efforts to create global rules are further hindered by digital nationalism and the strategic exploitation of cyberspace for espionage and influence operations, which erode good faith negotiations.

Sovereignty and jurisdiction issues: Sovereignty in cyberspace remains a contested concept. At the same time, states assert jurisdiction over data and infrastructure within their borders, and cross-border data flows and extraterritorial cyber operations muddy legal interpretations. Jurisdictional conflicts arise in scenarios such as data localization laws clashing with multinational cloud services, or cybercrime investigations requiring cross-border cooperation without precise legal mechanisms. The Tallinn Manual offers guidance on applying international law to cyber conflicts, but its interpretations are non-binding and often controversial. Sovereignty debates increasingly intersect with national security, digital economy, and human rights, making consensus elusive and usually politicized.

Chapter 10: International Cybersecurity Framework and Alliances

NATO and its cyber defense posture: NATO has steadily evolved its cyber defense posture, recognizing cyberspace as a domain of operations alongside land, sea, air, and space. The 2016 Warsaw Summit formally declared that a cyberattack on a member state could trigger Article 5, NATO's collective defense clause. This has significant strategic implications, particularly as attribution remains challenging. NATO has focused on resilience, capability building, and intelligence sharing, while fostering cooperation with the EU and private sector. However, disparities in member states' cyber capabilities and politics will continue to pose integration challenges. Exercises like Locked Shields, organized by NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), play a pivotal role in operational readiness.

EU initiatives and challenges: The European Union has made substantial efforts to harmonize cybersecurity across member states through initiatives like the EU Cybersecurity Act and the NIS2 Directive. The European Union Agency for Cybersecurity (ENISA) coordinates efforts to enhance threat intelligence, certification schemes, and cyber crisis response. Yet, operational cohesion, resource disparities, and bureaucratic fragmentation remain. Moreover, Europe's dependence on non-EU technologies raises strategic vulnerabilities, prompting initiatives like the GAIA-X project to foster digital sovereignty. While political will is growing, translating policy frameworks into actionable, interoperable defenses remains a critical hurdle.

Bilateral cyber pacts (US-Israel, China-Russia, etc.): Bilateral cyber agreements are crucial in shaping global cyber norms and strategic alignments. The U.S.-Israel partnership emphasizes intelligence sharing, joint R&D, and capacity building, reflecting a shared interest in technological edge and countering cyber threats from hostile states and non-state actors. Conversely, the China-Russia cyber pact focuses on mutual non-aggression in cyberspace and coordinated approaches to information control, underlining an authoritarian vision of cyber sovereignty. These bilateral arrangements reveal competing blocs in cyber diplomacy, often circumventing multilateral gridlock and risking global governance fragmentation.

The role of non-state actors (tech companies, NGOs): Non-state actors are increasingly influential in cybersecurity diplomacy. Tech giants like Microsoft and Google possess capabilities and data that rival nation-states, making them essential partners in threat detection and mitigation. Initiatives like the Cybersecurity Tech Accord and Microsoft's Digital Geneva Convention proposal reflect corporate efforts to influence norms. NGOs and civil society advocate for privacy, freedom of expression, and accountability, often serving as watchdogs and policy contributors. Integrating non-state actors complicates traditional diplomacy but offers agility and innovation, essential for addressing fast-moving cyber threats.

Chapter 11: The Global Cyber Arms Race and Power Projection

11.1 AI, Quantum Computing, and Next-Generation Warfare

This section highlights a transformative shift in warfare paradigms driven by the convergence of three frontier technologies: Artificial Intelligence (AI), Quantum Computing, and Cyber Capabilities. Together, these elements disrupt conventional timelines, decision-making processes, and the strategic balance of power.

- **AI in Warfare**:Artificial intelligence enables rapid data processing and autonomous decision-making, revolutionizing modern warfare, especially on the offensive front. In cyber operations, AI systems can scan vast networks for vulnerabilities, craft highly tailored exploits, and launch coordinated attacks with minimal human intervention. These systems can penetrate defenses faster than traditional methods and dynamically adapt to changing conditions, including rerouting attacks or modifying payloads in real time. AI can also automate phishing, social engineering, and malware propagation at scale, increasing the speed and precision of cyber assaults. On a broader scale, AI-generated deepfakes and synthetic media can be used offensively to sow discord, impersonate leaders, or fabricate events amplifying disinformation and psychological operations that destabilize societies from within. Moreover, autonomous weapons and drones, guided by AI, can be deployed for precision strikes or area denial with limited oversight, raising the risk of preemptive or disproportionate use in volatile situations. Together, these capabilities make AI not just a tool for defense, but a powerful force multiplier for offensive cyber and kinetic operations.

- **Quantum Threats to Cryptography:** Quantum computing poses a profound and potentially existential threat to contemporary cryptographic systems such as RSA and Elliptic Curve Cryptography (ECC). These encryption methods, which underpin much of today's secure communication, rely on the computational difficulty of problems like prime factorization and discrete logarithms challenges that classical computers struggle with but which quantum algorithms, such as Shor’s algorithm, can solve exponentially faster. Once scalable, fault-tolerant quantum machines become a reality, adversaries could decrypt previously secure data in moments, undermining the entire digital trust framework across governments, financial systems, and critical infrastructure. This looming threat is accelerating the global push toward post-quantum cryptography (PQC) encryption schemes designed to resist quantum attacks. However, the transition is asymmetric and uneven. Nations or actors that reach effective quantum decryption capabilities ahead of others could gain a significant and potentially unassailable intelligence advantage,

making this not just a technological race but a matter of national security and global power balance.

- **Convergence Risks: AI, Quantum, and Cyberwarfare:** The convergence of artificial intelligence and quantum technologies within the domain of cyberwarfare is creating an increasingly complex and opaque threat landscape. AI-driven advanced persistent threats (APTs) are becoming more autonomous, adaptive, and capable of evading traditional detection mechanisms. When paired with quantum-enabled decryption or sensing capabilities, such attacks could become faster, stealthier, and more devastating targeting vital infrastructure such as electrical grids, water systems, or transportation networks. This fusion significantly complicates attribution, eroding the ability to trace attacks back to their origin with confidence and thereby weakening conventional deterrence frameworks. Furthermore, the rapid pace of development and deployment often surpasses the creation of adequate regulatory, legal, or ethical safeguards. This regulatory lag increases the likelihood of strategic miscalculations, accidental escalation, or the normalization of covert digital aggression—pushing global cybersecurity toward a state of chronic instability.

The battlefield is shifting from physical to algorithmic, where milliseconds matter more than manpower. A new arms race is not only about weapons but about who controls the fastest, most intelligent machines.

11.2 Cyber Arms Market

The Cyber arms market is an opaque and decentralized ecosystem that challenges conventional distinctions between state and non-state actors. Unlike traditional arms markets subject to treaties, export controls, and global oversight the cyber domain operates in the shadows, where tools are traded with little regulation, anonymity is the norm, and attribution is deliberately obscured. This digital battleground is now a central front in global power struggles.

- **Commoditization of Offensive Tools:** The commoditization of advanced cyber weapons has accelerated the global cyber arms race. Sophisticated tools once restricted to elite intelligence agencies are now widely accessible. The leak of the NSA's EternalBlue exploit, later weaponized in global attacks like WannaCry and NotPetya, exemplifies how top-tier capabilities can escape containment and proliferate. Today, exploit trading platforms, dark web marketplaces, and private brokers routinely offer zero-day vulnerabilities and ready-to-use malware to the highest bidder. This democratization empowers not only nation-states, but also criminal syndicates, hacktivist groups, and lone actors, fundamentally altering the landscape of asymmetric warfare.

- **Rise of Cyber Mercenaries and Proxy Actors:** The growing role of cyber mercenaries private companies or individuals selling offensive capabilities adds further complexity. Firms such as NSO Group (creator of Pegasus spyware) demonstrate how advanced surveillance tools are commodified and exported to governments with minimal oversight. These tools have been linked to surveillance of journalists, activists, and political opponents across multiple continents. Other actors like DarkMatter (UAE) or Hacking Team (Italy) illustrate how offensive expertise is being privatized and outsourced, blurring lines of accountability and legality. These proxies provide governments with plausible deniability while offering devastating capabilities that rival state-developed cyber weapons.
- **State-Sponsored Operations and Outsourcing:** Nations increasingly rely on a hybrid model of in-house operations and external contractors to conduct offensive cyber campaigns. This strategy not only reduces cost and increases flexibility but also serves to muddy attribution, making it harder for victims and observers to identify the real perpetrator. However, this decentralization comes with risks: states can lose operational control, miscalculate escalation thresholds, or inadvertently enable reckless actions by loosely affiliated groups.

Specific countries like Russia, China, Iran, and North Korea are among the most active and notorious players in the cyber arms race. Russia's GRU-linked units have been tied to major operations such as the DNC hack and *NotPetya*. China's APT groups, particularly APT10 and APT41, have conducted sweeping industrial espionage campaigns. North Korea's Lazarus Group has targeted financial institutions to generate revenue under sanctions, while Iran's Charming Kitten and other groups have engaged in regionally focused espionage and disruption. Meanwhile, Western powers like the United States, Israel, and the United Kingdom maintain formidable capabilities, often operating through clandestine or allied frameworks (e.g., Five Eyes) and increasingly emphasizing cyber deterrence.

Cyberweapons are now as portable and versatile as firearms but invisible, untraceable, and scalable. The erosion of the state's monopoly on digital violence undermines traditional security doctrines.

11.3 Ethics, Escalation Risks, and Global Cyber Stability

This section touches on the underdeveloped and highly volatile ethical framework surrounding cyber conflict. Unlike traditional warfare, which has well-established norms (e.g., Geneva Conventions), cyber warfare remains in a normative vacuum.

- **Lack of Proportionality**: Many cyber operations disproportionately affect civilians targeting hospitals, water systems, or financial infrastructure. These actions, while non-lethal, can be catastrophic. The principle of distinction separating civilians from military targets is frequently violated, either by design or due to the interconnected nature of digital systems.

- **Escalation Dynamics**: The invisible and ambiguous nature of cyber attacks means that states may misinterpret incidents as acts of war or struggle to distinguish between espionage and sabotage. False flag operations, AI-generated misinformation, or bot-driven public opinion manipulation can escalate tensions rapidly without clear attribution.

- **Confidence-Building Measures (CBMs)**: International efforts like the UN's Group of Governmental Experts (GGE) or the Tallinn Manual attempt to build consensus on norms, but geopolitical mistrust often stymies progress. States hesitate to reveal capabilities or doctrines, fearing it would undermine strategic advantages.

- **Transparency vs. National Security**: There’s a trade-off between revealing doctrines for confidence-building and preserving secrecy for operational effectiveness. The absence of cyber equivalents to nuclear “red phones” or hotlines heightens the chance of conflict spiraling unintentionally.

In the cyber domain, silence can be deafening when rules are unclear and communications are covert, a single keystroke can ignite geopolitical fires.

Part IV: Innovations and Cyber Strategy

Chapter 12: The Private Sector as a Cyber Power

Major technology companies such as Microsoft, Amazon, Google, Apple, and Meta are central in shaping the global cybersecurity landscape. These firms act as both guardians defending vast digital infrastructures and gatekeepers, setting industry standards and norms. Microsoft, for instance, operates one of the largest threat intelligence networks in the world and has developed industry-leading solutions through its Defender suite and Security Copilot AI tools. Amazon Web Services (AWS) secures critical cloud infrastructure used by governments and enterprises alike, while Google's Chronicle and Mandiant (acquired in 2022) provide advanced incident response and threat detection capabilities. Apple leads in consumer security and privacy innovation through technologies like hardware encryption and biometric authentication.

These companies invest billions of dollars annually in cybersecurity R&D, establishing sophisticated Security Operations Centers (SOCs) and collaborating globally to detect and neutralize threats often identifying major vulnerabilities before governments are even aware. Their scale and resources make them indispensable to modern cyber defense. However, their dominance also raises important concerns about accountability, data sovereignty, and competitive fairness, especially when critical infrastructure and sensitive user data are concentrated in just a few hands. Their centrality makes them high-value targets, with breaches having systemic, global ripple effects.

Startups, Venture Capital, and the Innovation Ecosystem

Cybersecurity innovation also thrives within the startup ecosystem, where smaller firms pioneer emerging technologies like AI-powered anomaly detection, behavioral biometrics, quantum-resistant encryption, and zero-trust architectures. Companies such as CrowdStrike, SentinelOne, and Darktrace began as startups and have since become industry leaders. Venture capital is crucial in fueling this innovation, enabling rapid growth and scaling. Big Tech often acquires these startups. Google's acquisition of Mandiant and Amazon's interest in expanding cloud-native security services are recent examples of integrating their capabilities into larger ecosystems.

While this dynamic fosters rapid innovation, it can also concentrate technological power, potentially creating monocultures where a few dominant platforms introduce shared vulnerabilities with global impact.

Public-Private Partnerships and the Challenges Ahead

Effective cybersecurity also hinges on public-private collaboration, especially for protecting national critical infrastructure. Initiatives like the U.S. Cybersecurity Information Sharing Act (CISA) and the EU's NIS Directive aim to improve threat sharing and response coordination between governments and industry. However, these partnerships often face challenges including mismatched incentives, legal ambiguity, and bureaucratic inertia. Bridging these divides requires clear legal frameworks, mutual trust, and mechanisms that balance public interest with commercial imperatives. Ultimately, the interplay between Big Tech, startups, governments, and capital investors is redefining the future of cybersecurity. Ensuring a resilient and open digital ecosystem will depend on how these actors share responsibility, distribute power, and build trust across borders.

Chapter 13: Cyber Strategy in the Age of AI and Quantum Computing

AI-Driven Defense and Offense Strategies: AI transforms cybersecurity from reactive defense to predictive analytics. Defensive AI systems can autonomously hunt threats, respond in real time, and manage vast data streams. Conversely, offensive AI enables adaptive malware, large-scale social engineering, and real-time penetration testing. Dual-use dilemmas arise, demanding careful governance to prevent the militarization of AI in destabilizing ways.

Risks and Opportunities of Quantum Computing: Quantum computing holds the potential to revolutionize computational capabilities but poses existential risks to current cryptographic systems. While offering breakthroughs in optimization and machine learning, quantum computing could break RSA and ECC encryption, necessitating an urgent transition to quantum-resistant algorithms. The race is technological and strategic, as states seek quantum supremacy to ensure both offensive and defensive advantage.

Strategic Planning for Post-Quantum Cryptography: Preparing for the quantum era requires proactive planning, standardization, and transition strategies. Agencies like NIST are spearheading the development of post-quantum cryptographic standards, but widespread adoption lags. Governments and industries must inventory cryptographic assets, develop migration roadmaps, and invest in hybrid cryptographic solutions to bridge the transition period. Strategic foresight and interoperability are key to maintaining trust and resilience in the face of quantum disruption.

Chapter 14: Innovation Models from Global Cyber Hubs

Some of the world's smallest countries are punching well above their weight regarding cybersecurity and digital innovation. Estonia, Israel, Singapore, South Korea, and the Netherlands have each built robust cyber ecosystems that combine smart strategy, strong leadership, and bold innovation. Estonia, Israel, Singapore, South Korea, and the Netherlands stand out for building high-impact cyber ecosystems that others now look to as models. Each country brings a distinct approach shaped by its history, geography, and priorities, but they all are committed to innovation, resilience, and innovative governance.

14.1 Estonia: The Digital State Built on Resilience

Estonia's transformation into a digital powerhouse began after a major cyberattack in 2007. Instead of retreating, the country doubled down on digital governance. Today, Estonia offers one of the world's most advanced e-governance systems, where citizens can vote, access healthcare, and manage finances online.

Key strengths:

- Government-led digital services and identity systems
  Cyber defense is deeply integrated into national security.
  NATO Cooperative Cyber Defence Centre of Excellence in Tallinn

Estonia proves how a crisis can be a catalyst for becoming a global leader in digital resilience.

14.2 Israel: Where National Security Meets Cyber Startups

Israel's cyber strength flows directly from its defense strategy. Elite military units like Unit 8200 serve as a launchpad for talent and innovation. Veterans often transition into the private sector to found or join high-growth cybersecurity startups, creating a tight feedback loop between national defense and commercial success.

Key strengths:

- Close integration of military intelligence and tech innovation
  Vibrant cybersecurity startup ecosystem
- Massive foreign investment and export strength in cyber tech

Israel shows how national defense priorities can drive global leadership in cyber entrepreneurship and technology.

14.3 Singapore: Securing the Smart Nation

Singapore's goal of becoming the world's first brilliant nation includes cybersecurity as a core pillar. The government has made major investments in digital infrastructure and is positioning Singapore as a regional leader in cybersecurity training, research, and international collaboration.

Key strengths:

- Centralized cyber governance under the Cyber Security Agency (CSA)
- Strong legal and regulatory frameworks
- Focus on smart cities and secure urban infrastructure

Singapore is a model for integrating cyber policy into broader national development, particularly in urban technology and public services.

14.4 South Korea: Industrial Protection and Public-Private Unity

South Korea's digital economy depends heavily on its globally competitive electronics and automotive industries. The country's cybersecurity strategy is tightly focused on protecting industrial infrastructure and nurturing collaboration between government and private companies.

Key strengths:

- Strong industrial cybersecurity focus (manufacturing, telecom, energy)
- Rapid digital response infrastructure
- Emphasis on tech sovereignty and local capacity-building

South Korea highlights the role of cyber policy in protecting critical industries and maintaining economic competitiveness.

14.5 The Netherlands: The Global Connector

The Netherlands has taken on a unique role as a facilitator of international cybersecurity cooperation. The Hague is home to The Hague Security Delta, Europe's largest security cluster, and the country brings together governments, businesses, and research institutes to shape global cyber norms.

Key strengths:

- International diplomacy and cyber norm-building
- Strong cybersecurity R&D sector
- Public-private partnerships with a global outlook

The Netherlands is vital in bridging national strategies and global cooperation, offering a neutral, innovative space for dialogue and development.

Chapter 15: Strategic Frameworks and Doctrines in Cybersecurity

The evolution of cybersecurity from a technical concern to a core element of national and international security strategies marks a fundamental shift in how states conceptualize power, sovereignty, and conflict in the 21st century. This chapter explores how different geopolitical actors frame their cybersecurity postures, the divergence between military and civilian cyber doctrines, and the broader integration of cyber capabilities into grand strategy.

15.1 National Cyber Strategies: A Mirror of Geopolitical Identity

National cybersecurity strategies serve as internal governance tools and external signaling mechanisms, revealing underlying political ideologies, governance models, and strategic intentions.

- **United States:**
  U.S. cybersecurity strategy is shaped by its liberal democratic values and global security commitments. It emphasizes:

    - Deterrence by denial and punishment, combining cyber defenses with offensive capabilities and declaratory policies.
    - Public-private partnerships leverage the private sector's innovation and infrastructure, especially in critical areas like telecommunications and cloud services.
    - Resilience, with a focus on continuity of operations and rapid recovery from attacks.
      The U.S. also emphasizes international norms, pushing for a rules-based order in cyberspace and building coalitions through forums like the Quad, NATO, and bilateral cyber dialogues.

- **European Union:**
  The EU's cybersecurity posture is rooted in **regulatory governance and supranational coordination**, reflecting its identity as a normative power:

    - Regulatory harmonization through instruments like the NIS Directive and the GDPR.
    - Digital sovereignty aimed at reducing dependencies on non-EU tech platforms and asserting control over data flows.
    - Initiatives like ENISA and the EU Cybersecurity Act underpin cross-border cooperation. The EU blends technical regulation with

ethical considerations, positioning cybersecurity as part of a broader human-centric digital agenda.

- **China:**
  China's strategy is anchored in the concept of **cyber sovereignty**, linking cybersecurity with regime stability, economic modernization, and global influence:

    - State control over cyberspace, with the Cyberspace Administration of China acting as a regulator and ideological gatekeeper.
      Civil-military fusion, aligning private tech development with national security objectives.
    - Belt and Road digital initiatives, using infrastructure exports (e.g., 5G, surveillance tech) to extend influence and shape global cyber norms.
      China's model represents an authoritarian cyberspace doctrine, prioritizing control and strategic leverage over openness and multistakeholder governance.

These divergent national strategies are not merely administrative choices—they shape the **contours of international cyber diplomacy**, influencing norm-building, alliance formation, and technology governance worldwide.

15.2 Military vs. Civilian Cyber Doctrines: Dual Lenses of Power

The distinction between military and civilian cybersecurity doctrines reflects differing objectives, operational logics, and risk appetites. However, the boundaries between these spheres are increasingly porous.

- **Military Doctrine:**

    - Focused on cyber offense, including capabilities for preemptive strikes, disruption of enemy command and control, and psychological operations.
    - Integrated into hybrid warfare, cyberattacks accompany kinetic, informational, and economic strategies.
      Seen in doctrines like the U.S. Department of Defense's concept of "persistent engagement" and Russia's use of cyber as a non-kinetic force multiplier.
    - Often shrouded in secrecy, creating challenges for accountability and escalation management.

- **Civilian Doctrine:**

    - Prioritizes resilience, regulation, and risk management, particularly for critical infrastructure (e.g., energy, health, finance).
    - Focused on incident response, information sharing, and public trust.
    - Embedded in legal and constitutional frameworks, requiring transparency and oversight.
    - Includes broader societal elements such as digital literacy, public awareness campaigns, and norms against disinformation.

The growing **convergence** between civilian and military domains—especially in response coordination, information warfare, and infrastructure protection necessitates:

- **Role clarity**, to avoid duplication or overreach.
- **Institutional boundaries** are to uphold democratic norms and civil liberties.
- **Oversight mechanisms**, such as legislative scrutiny and judicial review.

Without such safeguards, there is a risk of **"mission creep"**, where security imperatives override democratic values under the guise of cyber defense.

Integrating Cyber into Grand Strategy: A Systemic Imperative

Cybersecurity can no longer be treated as a siloed or reactive function; it must be integrated into **national grand strategy** alongside traditional pillars like diplomacy, military power, and economic policy.

- **Strategic Integration:**

    - Cyber capabilities must inform foreign policy, enabling tools like cyber diplomacy, cyber sanctions, and digital capacity-building for allies.
    - They shape intelligence operations, enabling surveillance, espionage, and attribution.
    - Cyber strategy intersects with economic statecraft, influencing trade negotiations, tech alliances, and supply chain security.

- **Whole-of-Government Approach:**

    - Requires coordination across defense, intelligence, justice, energy, finance, and technology ministries.
    - Demands shared situational awareness, common threat frameworks, and unified response protocols.

- **Cyber-Informed Decision-Making:**
    - Decision-makers must understand the **strategic, legal, and ethical dimensions** of cyber operations, not just technical vulnerabilities.
    - National Security Councils or similar bodies must integrate cyber perspectives into **scenario planning and strategic foresight**.
- **Alignment with National Values:**
    - Cyber policies must reflect societal values of openness, sovereignty, or control.
    - Democracies face unique challenges in balancing **security and civil liberties**, especially when considering surveillance, encryption policy, and counter-disinformation efforts.

Ultimately, cyber strategy is not just about **protecting infrastructure;** it is about **shaping the future of power**. As cyberspace becomes a theater for great-power competition, ideological contestation, and technological disruption, strategic frameworks must evolve to remain adaptive, resilient, and grounded in a coherent vision of national interest.

Chapter 16: Cyber Resilience and Strategic Infrastructure Protection

Smart Infrastructure and IoT Security

The rapid expansion of Internet of Things (IoT) ecosystems and smart infrastructure ranging from connected cars and smart cities to industrial control systems and energy grids has radically altered cybersecurity. Each device connected to a network introduces a potential entry point for threat actors. These devices are often deployed without adequate security controls, exposing critical functions to remote exploitation. The fragmented nature of IoT standards creates significant challenges. With no universally accepted security framework, vendors prioritize time-to-market over robust protection. This results in inconsistencies across device firmware, update mechanisms, and data handling practices. Moreover, many IoT devices have limited computational power, restricting the implementation of traditional security solutions such as encryption and intrusion detection.

A comprehensive IoT security posture must encompass the following:

- Robust Device Authentication and Authorization: Ensuring that only authenticated devices communicate within the network, leveraging PKI (Public Key Infrastructure), digital certificates, or modern lightweight cryptographic protocols like DTLS or ECC.
- Secure Firmware Lifecycle Management: Regular firmware updates with cryptographic signing are critical for patching vulnerabilities and preventing malicious modifications.
- Network Segmentation and Micro-Segmentation: By isolating IoT networks from core business infrastructure, damage from a breach can be localized and contained.
- Behavioral Anomaly Detection: Continuous monitoring for deviations in device behavior can offer early indicators of compromise.
- Global Cooperation on Certification Standards: Just as Underwriters Laboratories (UL) certifies appliances for safety, the cybersecurity domain needs standardized third-party certifications to assure minimum security baselines for IoT devices.

Ultimately, the evolution of smart infrastructure demands a "zero trust" philosophy that assumes compromise and continuously verifies each component.

Resilience-by-Design Principles

The growing consensus among cybersecurity professionals is clear: breaches are inevitable. The measure of a secure system is not whether it can prevent all attacks, but whether it can withstand, adapt to, and recover from those attacks with minimal disruption. This paradigm is encapsulated in resilience-by-design, an engineering approach that treats resilience not as an add-on, but as a fundamental property of systems architecture.

Key Resilience-by-Design Components:

- **Secure Coding Practices:** Applications should be developed using input validation, least privilege, and memory safety to reduce exploitable bugs from inception.
- **Redundancy and Diversity:** System redundancy, both in hardware and software, ensures that a single point of failure does not compromise functionality. Diversity, such as using different software stacks across redundant systems, further protects against monoculture vulnerabilities.
- **Deception and Obfuscation Techniques:** Honeypots, honeytokens, and deception grids detect intrusions, delay attackers, and collect intelligence. Continuous Monitoring and Threat Intelligence Integration: Real-time telemetry combined with AI-driven analytics allows systems to quickly detect and respond to anomalies. Automated Response and Self-Healing Mechanisms: In advanced systems, autonomous response capabilities can isolate affected segments and initiate rollback or reconfiguration protocols in real-time.

Critically, resilience-by-design represents a philosophical shift: away from the fortress model of cybersecurity built on the illusion of impenetrability and toward adaptive, robust, and self-correcting architectures.

National Critical Infrastructure and Supply Chain Security

The security of national critical infrastructure energy grids, water systems, transportation networks, healthcare facilities, and financial institutions—is now directly tied to cybersecurity resilience. Recent events such as the Colonial Pipeline ransomware attack and disruptions to global chip manufacturing during the COVID-19 pandemic revealed how fragile and interconnected these systems are.

Supply Chain Threat Vectors:
Supply chain threats are particularly insidious because they exploit trust. Attackers can gain access at foundational levels through compromised hardware components, infected software updates (e.g., SolarWinds), or malicious insider actions. These threats are difficult to detect and mitigate post-factum, making proactive assurance and transparency vital.

Strategic Protective Measures Include:

- Rigorous Supply Chain Risk Assessments: Continuous evaluation of third-party vendors, security practices, ownership structures, and geopolitical affiliations.
- Zero-Trust Supply Chain Models: Ensuring no component, even from trusted partners, is inherently trusted without verification.
- Trusted Vendor Programs and National Certification: Developing national or multinational vetting programs for critical suppliers, akin to the U.S. Federal Acquisition Supply Chain Council (FASCC).
- Diversity and Strategic Redundancy: Avoiding overreliance on a single vendor or region, especially those under the jurisdiction of potentially adversarial states.
- Legislative and Policy Frameworks: Enacting regulations that require transparency, secure development practices, and incident reporting from suppliers of critical infrastructure components.

Moreover, national resilience requires public-private partnerships. Governments cannot protect infrastructure in isolation. Coordinated intelligence sharing, joint incident response capabilities, and cross-sector simulation exercises are essential to maintaining operational continuity.

Strategic Insights and Future Directions

- Cyber Resilience as a National Asset: In an era of hybrid warfare and geopolitical cyber competition, resilience is no longer just an IT concern but a pillar of national security and economic stability. Countries with high cyber resilience will have strategic advantages in deterrence, diplomacy, and defense. The Shift from Cybersecurity to Cyber Resilience: This subtle but essential shift acknowledges that perfect prevention is impossible, and that preparation, adaptability, and response are the new hallmarks of mature security ecosystems.
- Digital Sovereignty and Strategic Autonomy: Countries must evaluate the trade-offs between globalization and national autonomy. While global supply chains have driven economic efficiencies, they have also created systemic dependencies. Future strategies will favor trusted local manufacturing, sovereign cloud infrastructures, and open-source transparency.

- Resilience as a Competitive Advantage: Organizations that embed resilience from product design to operations will outperform in risk-sensitive industries. Investors, insurers, and regulators are beginning to evaluate resilience metrics alongside financial metrics.

Chapter 17: Future Scenarios and Strategic Foresight in Cyberspace

Scenario Planning for Strategic Cyber Futures

Scenario planning is a powerful strategic foresight tool that empowers policymakers to envision and navigate a range of plausible futures in cyberspace. As digital technologies evolve rapidly, and geopolitical, social, and economic forces intersect in complex ways, the ability to anticipate disruptive shifts becomes critical. Scenario planning involves constructing narrative-driven futures that span a spectrum from optimistic visions of globally interoperable and secure digital commons, where cooperation and norms govern behavior, to pessimistic outcomes characterized by fragmented, authoritarian-controlled, or militarized internets plagued by constant conflict. This method is not about predicting the future but preparing for it. By grappling with divergent possibilities, decision-makers can identify early warning signals, stress-test policies, and craft resilient adaptive strategies under a wide range of conditions. Scenario planning promotes institutional agility, helping organizations move beyond reactive responses to proactive, long-term thinking. Importantly, it encourages inclusive dialogue across sectors and disciplines, ensuring that diverse perspectives shape the cyber future.

Red Teaming, Wargaming, and Cyber Simulations

Traditional planning is insufficient in an era where cyber threats are asymmetric, unpredictable, and often stealthy. Red teaming, wargaming, and cyber simulations have become essential methods for exposing vulnerabilities, challenging assumptions, and enhancing institutional preparedness. These activities immerse participants in realistic adversarial scenarios, allowing them to simulate potential attackers' tactics, techniques, and procedures (TTPs), including nation-states, criminal syndicates, hacktivists, and insiders. Red teaming involves deliberately adopting an adversary’s mindset to identify system, process, and defense weaknesses. Wargaming extends this by modeling complex cyber conflict dynamics, often incorporating geopolitical, economic, and kinetic dimensions. Cyber simulations are training environments that foster coordination across government, industry, and civil society. Collectively, these exercises sharpen strategic thinking, promote a culture of proactive defense, and strengthen cross-functional collaboration. They also offer opportunities to evaluate the effectiveness of policies, communication flows, and crisis decision-making under stress.

Strategic Uncertainty and Decision-Making in the Cyber Era

Uncertainty is not just a feature of cyberspace it is its defining characteristic. The rapid pace of technological innovation, the opacity of attribution, the diversity of actors, and the constant evolution of threat landscapes create a decision-making environment marked by ambiguity and risk. In such a context, linear planning and rigid policy frameworks quickly become obsolete. Effective cyber governance requires decision-makers to adopt a mindset rooted in probabilistic reasoning and continuous learning. This includes scenario-based thinking, iterative policy design, and rapid feedback and adaptation mechanisms. It also demands investment in strategic foresight capabilities and interdisciplinary collaboration—blending technical expertise with legal, economic, and sociopolitical insights. By building institutional capacity for resilience and responsiveness, governments and organizations can better withstand shocks and seize emerging opportunities. In sum, navigating strategic uncertainty in cyberspace calls for a shift from control-oriented models to adaptive systems thinking. Institutions must become learning organizations able to anticipate, experiment, and evolve in the face of volatility.

Conclusion

Cyberspace today stands at the crossroads of opportunity and peril a powerful domain shaping economic growth, geopolitical rivalry, and social transformation. Yet it is equally a space riddled with risk. From decentralized criminal networks and ideologically driven cyberterrorists to state-sponsored operations and disinformation campaigns, threats in the digital domain are persistent, adaptive, and increasingly strategic. Cybercrime has evolved into a global ecosystem agile, commercialized, and deeply embedded in encrypted platforms and dark markets. Its impact is not only economic but strategic, eroding public trust, targeting critical infrastructure, and overwhelming law enforcement capabilities across borders. Cyberterrorism adds another layer of volatility, exploiting digital tools for radicalization, recruitment, and disruption, while remaining difficult to trace and counter. State-driven cyber warfare has emerged as a central element of modern conflict. Nations leverage cyberspace to pursue political objectives, shape public opinion, and weaken adversaries without traditional confrontation. As digital attacks become more precise and frequent, the line between espionage, sabotage, and war continues to blur.

These shared threats call for collective action. No single nation or entity can secure the digital sphere in isolation. Stronger international cooperation is essential not only through alliances and cybersecurity frameworks, but through meaningful diplomacy that can build norms, enable attribution, and hold malicious actors accountable. The absence of globally binding rules in cyberspace remains one of the greatest strategic vulnerabilities of our time. For states, the way forward lies in developing comprehensive cyber strategies that integrate defense, intelligence, law enforcement, and diplomacy. National resilience depends not only on securing networks, but on anticipating future threats, regulating critical technologies, and fostering strategic partnerships across sectors and borders.

The private sector, as steward of much of the world's digital infrastructure and innovation, bears equal responsibility. Businesses must prioritize cybersecurity as a strategic imperative, not a technical add-on embedding it into design, governance, and culture. Greater coordination with governments, investment in threat intelligence, and transparency in incident response are no longer optional, but essential. Looking ahead, the challenges will grow more complex. The rise of artificial intelligence, quantum computing, and autonomous systems will redefine the nature of both opportunity and risk. The pace of technological change demands foresight, adaptability, and above all, unity. Cyberspace is not a lawless frontier but it is still an unfinished one. Its future will be shaped by those who are willing to lead with clarity, cooperate with resolve, and innovate with security in mind. The stakes are no longer virtual; they are societal, geopolitical, and deeply human. Only by acknowledging this shared responsibility and acting on it can we hope to secure a stable and resilient digital future.

Bibliography

1. Abbate, J., Inventing the Internet, MIT Press, Cambridge, 1999.
2. Amazon Web Services, AWS Cloud Security Overview, https://aws.amazon.com/security/.
3. Armbrust, M., et al., ‘A View of Cloud Computing’, Communications of the ACM, 2010.
4. Ashton, K., ‘That “Internet of Things” Thing’, RFID Journal, 2009.
5. Bada, M. and Sasse, A., ‘Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?’, arXiv preprint arXiv:1901.02672, 2019.
6. Berners-Lee, T., Weaving the Web, HarperSanFrancisco, San Francisco, 1999.
7. Boyd, D.M. and Ellison, N.B., ‘Social Network Sites: Definition, History, and Scholarship’, Journal of Computer-Mediated Communication, 2007.
8. Brundage, M., et al., The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, Future of Humanity Institute, Oxford, 2018.
9. Castells, M., The Internet Galaxy: Reflections on the Internet, Business, and Society, Oxford University Press, Oxford, 2001.
10. Cerf, V. and Kahn, R., ‘A Protocol for Packet Network Intercommunication’, IEEE Transactions on Communications, 1974.
11. Chesney, R. and Citron, D., ‘Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security’, California Law Review, vol. 107, no. 6, 2019, pp. 1753–1819, https://doi.org/10.15779/Z38RV0D67C.
12. Clarke, R.A. and Knake, R.K., Cyber War: The Next Threat to National Security and What to Do About It, Ecco, New York, 2010.
13. Comer, D.E., Internetworking with TCP/IP Volume One, 6th edn, Pearson, Boston, 2018.
14. Creemers, R., ‘Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century’, Journal of Contemporary China, vol. 26, no. 103, 2017, pp. 85–100.
15. CrowdStrike, Global Threat Report 2023, https://www.crowdstrike.com/resources/reports/.
16. Darktrace, Cyber AI Report 2023, https://www.darktrace.com/en/resources.
17. Deibert, R., Black Code: Surveillance, Privacy, and the Dark Side of the Internet, Signal, Toronto, 2013.
18. European Commission, Directive on Security of Network and Information Systems (NIS2), 2022, https://digital-strategy.ec.europa.eu.
19. European Union Agency for Cybersecurity (ENISA), EU Cybersecurity Act, 2019, https://www.enisa.europa.eu/topics/csirt-cert-services/eu-cybersecurity-act.
20. Floridi, L., ‘On Human Dignity as a Foundation for the Right to Privacy’, Philosophy & Technology, vol. 29, 2016, pp. 307–312, https://doi.org/10.1007/s13347-016-0220-8.

21. Google Cloud, Chronicle Security Operations Suite Overview, https://cloud.google.com/chronicle.
22. Greenberg, A., Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers, Doubleday, New York, 2019.
23. Hafner, K. and Lyon, M., Where Wizards Stay Up Late: The Origins of the Internet, Simon & Schuster, New York, 1996.
24. Harari, Y.N., 21 Lessons for the 21st Century, Spiegel & Grau, New York, 2018.
25. Harcourt, B.E., Exposed: Desire and Disobedience in the Digital Age, Harvard University Press, Cambridge, 2015.
26. Harknett, R.J. and Fischerkeller, M.P., 'Persistent Engagement and the Future of Cyber Strategy', Survival, vol. 60, no. 1, 2018, pp. 127–142.
27. Healey, J., A Fierce Domain: Conflict in Cyberspace, 1986 to 2012, Cyber Conflict Studies Association, 2011.
28. Internet Society, Internet Infrastructure, 2021.
29. Isaacson, W., Steve Jobs, Simon & Schuster, New York, 2011.
30. Kello, L., The Virtual Weapon and International Order, Yale University Press, New Haven, 2017.
31. Kurose, J.F. and Ross, K.W., Computer Networking: A Top-Down Approach, 8th edn, Pearson, Boston, 2021.
32. Lee, R.M., Assante, M.J. and Conway, T., ICS Cybersecurity: Case Studies and Best Practices, SANS Institute, 2016.
33. Leiner, B.M., et al., 'A Brief History of the Internet', ACM SIGCOMM Computer Communication Review, 2009.
34. Libicki, M.C., Cyber Deterrence and Cyber War, RAND Corporation, Santa Monica, 2009.
35. Mandiant, M-Trends Report 2023, https://www.mandiant.com/resources/m-trends.
36. Maurer, T., Cyber Mercenaries: The State, Hackers, and Power, Cambridge University Press, Cambridge, 2018.
37. Microsoft, Digital Defense Report 2023, https://www.microsoft.com/en-us/security/business/digital-defense-report.
38. Mockapetris, P., Domain Names—Concepts and Facilities (RFC 1034), 1987.
39. National Cyber Security Centre (NCSC), Connected Places Cyber Security Principles, UK Government, London, 2022.
40. National Institute of Standards and Technology (NIST), Post-Quantum Cryptography Standardization Project, U.S. Department of Commerce, 2023, https://csrc.nist.gov/Projects/post-quantum-cryptography.
41. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), https://ccdcoe.org/.
42. Nye, J.S., The Future of Power, PublicAffairs, New York, 2011.
43. O'Neil, C., Weapons of Math Destruction, Crown Publishing Group, New York, 2016.

44. Ottis, R., ‘Analysis of the 2007 Cyber Attacks Against Estonia’, Cooperative Cyber Defence Centre of Excellence, 2008.
45. Pennycook, G. and Rand, D.G., ‘Fighting Misinformation on Social Media Using Crowdsourced Judgments of News Source Quality’, Proceedings of the National Academy of Sciences, vol. 116, no. 7, 2019, pp. 2521–2526.
46. Paul, C. and Matthews, M., The Russian “Firehose of Falsehood” Propaganda Model, RAND Corporation, Santa Monica, 2016.
47. Rid, T., Cyber War Will Not Take Place, Oxford University Press, Oxford, 2013.
48. Rosen, C., ‘The Myth of Multitasking’, The New Atlantis, 2008.
49. Royal United Services Institute (RUSI), Scenario Planning for Cybersecurity, https://rusi.org/.
50. SANS Institute, Building and Operating a Modern SOC, Shackleford, D., 2021.
51. Schneier, B., Click Here to Kill Everybody: Security and Survival in a Hyper-connected World, W. W. Norton & Company, New York, 2018.
52. SentinelOne, Annual Threat Intelligence Report, https://www.sentinelone.com/labs/.
53. Singer, P.W. and Friedman, A., Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, Oxford, 2014.
54. Starosielski, N., The Undersea Network, Duke University Press, Durham, 2015.
55. Stouffer, K., Falco, J. and Scarfone, K., Guide to Industrial Control Systems (ICS) Security (NIST SP 800-82), National Institute of Standards and Technology, 2011.
56. Sultan, N., ‘Cloud Computing for Education: A New Dawn?’, International Journal of Information Management, vol. 30, no. 2, 2010, pp. 109–116.
57. Tapscott, D. and Tapscott, A., Blockchain Revolution, Portfolio, New York, 2016.
58. Tanenbaum, A.S. and Wetherall, D.J., Computer Networks, 5th edn, Pearson, Boston, 2011.
59. The Hague Security Delta, Cyber Security for the Future, https://www.thehaguesecuritydelta.com/.
60. Turkle, S., Alone Together: Why We Expect More from Technology and Less from Each Other, Basic Books, New York, 2011.
61. U.S. Congress, Cybersecurity Information Sharing Act (CISA), 2015, https://www.congress.gov/bill/114th-congress/senate-bill/754.
62. U.S. Department of Defense, Cyber Strategy, 2015.
63. U.S. Department of Defense, DoD Cyber Strategy, 2023, https://media.defense.gov/2023.
64. Vosoughi, S., Roy, D. and Aral, S., ‘The Spread of True and False News Online’, Science, vol. 359, no. 6380, 2018, pp. 1146–1151.
65. Wardle, C. and Derakhshan, H., Information Disorder, Council of Europe Report, 2017.

66. Weber, R.H., ‘Internet of Things – New Security and Privacy Challenges’, Computer Law & Security Review, vol. 26, no. 1, 2010, pp. 23–30.
67. West, D.M., The Future of Work: Robots, AI, and Automation, Brookings Institution Press, Washington, D.C., 2018.
68. World Economic Forum, The Global Risks Report 2016, Geneva, 2016.
69. World Economic Forum, Global Cybersecurity Outlook 2024, Geneva, 2024, https://www.weforum.org/.
70. Zegart, A.B., ‘Spies, Lies, and Algorithms: The History and Future of American Intelligence’, Foreign Affairs, 2022.
71. Zuboff, S., The Age of Surveillance Capitalism, PublicAffairs, New York, 2019.

About the Author

I am a cyber intelligence expert with over a decade of experience across diverse sectors, including academia, high-tech, military, and law enforcement. My core expertise lies in intelligence strategy, collection, research, and analysis, specializing in leading Cyber HUMINT operations targeting criminal and terrorist activities in cyberspace. My research interests center on cyber geopolitics and conflict dynamics. I have also trained numerous civilian analysts, military personnel, and law enforcement officers in Deep and Dark Web environments, cyber intelligence collection, and Cyber HUMINT methodologies.

