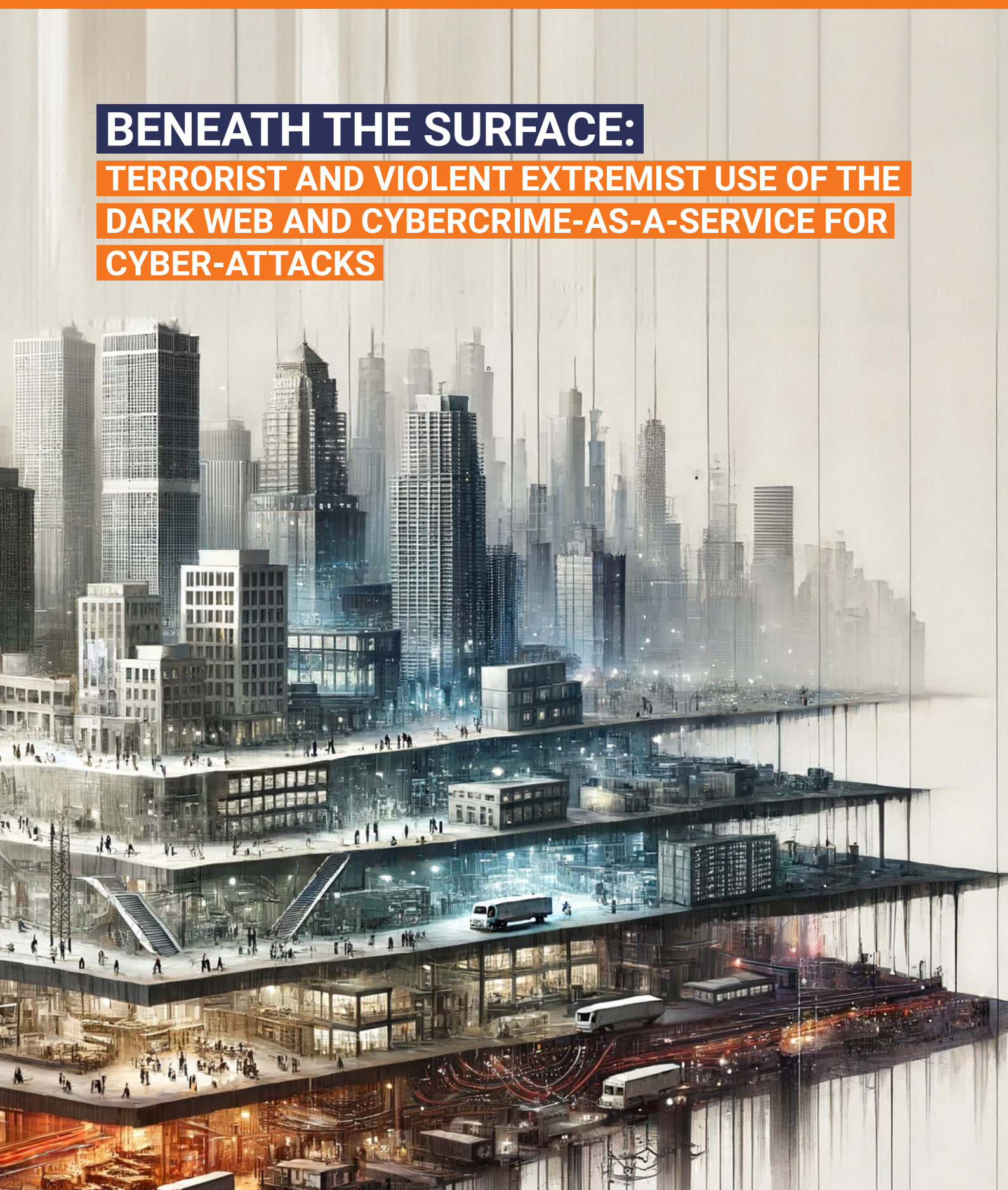UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

unicri
United Nations
Interregional Crime and Justice
Research Institute

BENEATH THE SURFACE:
TERRORIST AND VIOLENT EXTREMIST USE OF THE DARK WEB AND CYBERCRIME-AS-A-SERVICE FOR CYBER-ATTACKS

BENEATH THE SURFACE:

TERRORIST AND VIOLENT EXTREMIST USE OF THE DARK WEB AND CYBERCRIME-AS-A-SERVICE FOR CYBER-ATTACKS

Disclaimer

The opinions, findings, conclusions and recommendations expressed herein do not necessarily reflect the views of UNICRI, UNOCT or contributory organizations, and do not imply any endorsement. The content of this publication may be quoted or reproduced in part, provided that the source of information is acknowledged. UNICRI and UN-OCT would like to receive a copy of the document in which this publication is used or quoted.

The designation employed and presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations and UNICRI, concerning the legal status of any country, territory, city or area of its authorities, or concerning the delimitation of its frontiers or boundaries.

Acknowledgements

Copyright

Foreword

As the threat landscape continues to evolve throughout the digital age, the intersection of terrorism, violent extremism conducive to terrorism, and cybercrime presents an increasingly formidable challenge to global security. The misuse of the Internet and other communication technologies has long raised significant concerns, prompting concerted efforts to understand and combat these multifaceted threats. However, it is crucial to recognize the dual nature of those technological advancements. While these technologies are exploited by malicious actors for nefarious purposes, they also offer significant benefits for counter-terrorism efforts. Advanced data analytics, digital forensics and the use of open-source intelligence, conducted in line with human rights standards and the rule of law, can empower law enforcement agencies to track, predict, and thwart terrorist activities with precision and efficiency. From the perspective of counter-terrorism, the United Nations Global Counter-Terrorism Strategy, and its successive reviews, underscore the critical importance of addressing both the challenges and opportunities emanating from cyberspace.

This report is a collaborative endeavour of the United Nations Office of Counter-Terrorism (UNOCT), through its United Nations Counter-Terrorism Centre (UNCCT) and the United Nations Interregional Crime and Justice Research Institute (UNICRI), drawing on the expertise of the private sector, law enforcement agencies, and cybersecurity professionals in an effort to shed light on the intricate relationship between terrorism, violent extremism conducive to terrorism, and cybercrime. Its aim is to provide insights and analysis to inform strategies and capacity-building initiatives to counter the convergence of terrorism and cyber threats in the dark corners of the Internet.

At its core, this report sheds light on the phenomenon of cybercrime-as-a-service, exploring how terrorists, and cybercriminals leverage the dark web to procure tools and services for nefarious purposes. In doing so, it highlights the challenges faced by law enforcement agencies in attributing cyber-enabled threats emanating from the dark web and underscores the need for enhanced investigative capabilities. While the dark web serves as an important hub for cybercrime-as-a-service, the report also emphasizes the broader emerging cybercrime underground and the central role of encrypted platforms in facilitating communication and coordination among malicious actors.

The findings of this report challenge the prevailing assumptions about the cyber capabilities of terrorist groups, demonstrating how collaboration with cybercriminal elements not only blurs traditional distinctions but also amplifies the threat of more advanced cyber-enabled attacks. Addressing the emerging nexus between terrorism, violent extremism conducive to terrorism, and cybercrime necessitates a coordinated and multifaceted response. By fostering collaboration, sharing expertise, and bolstering investigation capabilities, stakeholders can effectively mitigate the risks posed by cybercrime-as-a-service and strengthen counter-terrorism efforts in the digital domain.

As we navigate the complexities of the modern security landscape, we trust that this report will serve as a call to action to confront these digital challenges with resolve and determination, safeguarding the integrity and security of cyberspace for present and future generations. Together, let us rise to the occasion and chart a course towards a safer, more secure digital future.

Vladimir Voronkov
Under-Secretary-General
United Nations Office of Counter-Terrorism
Executive Director
United Nations Counter-Terrorism Centre

Leif Villadsen
Acting Director
United Nations Interregional Crime and
Justice Research Institute

Executive Summary

The convergence of terrorism and violent extremism conducive to terrorism (hereafter violent extremism) with cybercrime presents a formidable challenge. The United Nations Global Counter-Terrorism Strategy (A/RES/77/298), and its successive reviews, have expressed concern over the misuse of the Internet and other information and communications technologies by terrorist groups and individuals, yet the intricacies of the relationship between terrorism and violent extremism on the one hand and cybercriminality on the other remain nebulous – particularly in the darker corners of the Internet.

This report – a collaboration between the United Nations Counter-Terrorism Centre (UNCCT) at the Office of Counter-Terrorism (UNOCT) and the United Nations Interregional Crime and Justice Research Institute (UNICRI) – investigates the complex interplay between these two worlds, focusing in on the cybercrime-as-a-service phenomenon that has emerged on the dark web over the course of the past two decades. The report aims to provide valuable insights on this topic for a diverse audience, including policymakers, law enforcement, cybersecurity professionals, and researchers. In light of this diverse audience, the report is structured to allow for diverse readers to access the findings by providing an introduction to the necessary technical elements of this topic, before delving in deeper at a more substantive level in key aspects.

A central theme of the report is the rise of cybercrime-as-a-service and its role in revolutionizing the cybercrime landscape. This model lowers the barriers to entry, enabling malicious actors to access a broad array of tools, resources, and expertise and facilitating them to conduct more complex cyber-attacks with greater ease. Cybercrime-as-a-service also facilitates collaboration among individuals and groups, increasing the scale and impact of cyber-attacks, while also making them harder to detect. The report posits that, in addition to transforming the cybercrime landscape, cybercrime-as-a-service represents a paradigm shift in terms of cyber-enabled terrorism. The advent and continued growth of cybercrime-as-a-service challenges the long-established belief that the threat of advanced cyber-enabled terrorist attacks is low because these groups and individuals possess limited cyber-attack capabilities.

The dark web is a crucial platform in terms of cybercrime-as-a-service and the entire cybercrime ecosystem, serving as a hub for the exchange of cybercrime services. The report, however, also emphasizes an expansion of this ecosystem, with malicious actors increasingly utilizing encrypted communications platforms to gather, communicate, sell unlawfully obtained assets, and acquire criminal services and products in what is perhaps best termed as a criminal or cybercrime underground.

In seeking to highlight the perceived nuanced and intricate connections between terrorism, violent extremism and cybercrime, several challenges were encountered in this study. Chief among these is the difficulty in defining and categorizing these threats due to the lack of universally accepted definitions. The investigation at the heart of this study was also significantly impacted by the issue of attribution and definitively understanding the identity of threat

actors involved in an attack and their motivations. The collective nature of some groups further complicates the threat landscape, as these collectives enable anyone with cyber skills to contribute to attacks, making it challenging for law enforcement agencies to attribute and assess threats accurately.

Despite this, evidence gathered clearly indicates that threat actors motivated by a belief system rather than purely financial considerations are engaged with cybercriminal elements in the dark web and the broader cybercrime underground in the context of cybercrime-as-a-service. Examining these threat actors reveals how a convergence through cybercrime-as-a-service can increases the risk of terrorism and violent extremism-related cyber-attacks.

The report therefore emphasizes the importance of recognizing a broader landscape in the cybercriminal underground, where threat actors motivated by financial and other considerations operate, and consequently prompts a reassessment of existing assumptions of the cyber capabilities of threat actors, including those engaged in terrorism and violent extremism. In this regard, the report serves as a call for collective reflection on the threat of cyber-enabled terrorism and heightened emphasis on coordination to facilitate the development of a more complete threat picture of terrorism and violent extremism in the dark web and on encrypted communication platforms. To this end, the report provides a series of recommendations aimed at policymakers, law enforcement, cybersecurity professionals, and researchers, that stress the need for collaborative action and enhancing cybercrime investigation capabilities to address the convergence of terrorism and violent extremism with cybercriminality. Importantly, the report calls for the establishment of comprehensive frameworks to foster closer cooperation and shared expertise between counter-terrorism units, cybercrime investigators, and technical specialists to advance understanding and guide investigative capabilities. Recognizing the sensitivities that come with this and that this may create conditions that lead to interferences with human rights, the report recommends adopting proactive and human rights-compliant measures to effectively mitigate risks and bolster counter-terrorism efforts in the digital domain.

The recommendations contained in this report, as well as its overall findings from the study, are intended to inform strategic initiatives and strengthen counter-terrorism efforts, safeguarding cyber- space for present and future generations.

Table of Contents

Key Terms and Concepts

Cyber-Attack – Malicious attempts to exploit vulnerabilities in information systems or physical systems in cyberspace and to damage, disrupt or gain unauthorized access to these systems.[1]

Cybercrime-as-a-Service – An organized cybercrime model where cybercriminals sell their tools, expertise, and services to others.[2] This includes various subsets or categories such as Distributed-Denial-of-Service (DDoS)-as-a-Service, Ransomware-as-a-Service, Malware-as-a-Service, Fraud-as-a-Service, among others.

Cybercrime Underground - Refers to the virtual spaces, techniques, platforms, and tools used by threat actors to gather, communicate, sell their unlawfully obtained assets, and acquire criminal services and products.[3]

Darknet – Part of the Internet, otherwise known as overlay networks, accessed using specific software, such as the Tor browser, which provides anonymity to users by encrypting their internet traffic and routing it through a series of servers. Darknets are not inherently criminal or illegal in nature.

Dark Web – The many hidden criminal websites and services hosted on darknet networks to intentionally obscure access. Unlike darknets which are not in themselves criminal, the dark web is often associated with illicit activities, including the sale of drugs, weapons, stolen data, and other illegal goods and services.

Deep Web – The part of the Internet that is not indexed by traditional search engines like Google, Bing and Yandex and consists of content that requires specific credentials, permissions, or direct uniform resource locators (URL) to access. It encompasses a wide range of content, such as password-protected websites, online databases, private networks, academic and scientific resources, legal documents, subscription-based services, and more.[4]

Encrypted Communication Platforms – Secure communication pathways, such as platforms like Telegram, Rocket Chat, and Discord, where data is transformed into unreadable code to prevent unauthorized access. Only individuals with the appropriate decryption keys can decipher and access the original information. These channels enhance the privacy and security of digital communications.

---

1   https://www.iso27001security.com/html/glossary.html
2   https://heimdalsecurity.com/blog/what-is-cybercrime-as-a-service-caas/
3   https://www.forbes.com/sites/forbestechcouncil/2023/05/10/an-executives-guide-to-the-cybercrime-underground/
4   https://www.kaspersky.com/resource-center/threats/deep-web

Context and Background

The Two Sides of the Digital World

Connectivity and the broader digital realm play a central role in shaping the landscape of modern society. Throughout the 21st Century, the process of digitalization has brought immense benefits by expanding economic and livelihood opportunities for a significant and growing portion of the global population. It has provided enhanced access to information and services for individuals worldwide who might otherwise have lacked such opportunities, connecting people across diverse geographies and cultures, and offering new means to advocate, defend, and exercise human rights. The Internet has been at the heart of this digital transformation. According to the International Telecommunications Union (ITU), as of 2023, 67 per cent of the world's population – amounting to 5.4 billion people – were online and connected through cyberspace.[5] Including the remaining 33 per cent and closing gender digital divide,[6] which remains substantial in some regions and low-income countries,[7] present some challenges but, more significantly, unique opportunities to realize development goals, such as those outlined in the 2030 Agenda for Sustainable Development, and to unify humanity.[8]

However, beneath the surface of these significant positive contributions, there is an alternate digital landscape harbouring concealed threats. One of the layers is the enigmatically termed 'dark web' – a clandestine part of the Internet not accessible through regular search engines or browsers, intentionally hidden and requiring specialized software to enter. Constituting an estimated 5 per cent of all the Internet content,[9] the nature and characteristics of this domain offer heightened levels of anonymity especially appealing to malicious actors. As a consequence, numerous illegal activities thrive here. Illicit marketplaces serve as hubs for trafficking in illicit drugs, weapons, counterfeits, and various contraband, employing cryptocurrencies to obscure transactions. Meanwhile, other malicious actors exploit this dark ecosystem for cybercrime – hacking, distributed denial-of-service, ransomware, phishing, selling stolen information, and other crimes. Since its inception, the dark web ecosystem has evolved into a notorious underworld, presenting substantial challenges to law enforcement agencies worldwide.

---

5   https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use/

6   https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-the-gender-digital-divide/

7   Ibid. According to the ITU, in Africa only 32% of women have access to the Internet compared to 42% of men, while in the Arab States 64% of women and 74% of men can access the Internet. In low-income countries the disparity is particularly notable, with only 20% of women having access to the Internet compared to 34% of men. This highlights how multiple forms of discrimination can intersect.

8   For more on how digitalization can advance sustainable development, see ITU - Digital technologies to achieve the UN SDGs: www.itu.int/en/mediacentre/backgrounders/Pages/icts-to-achieve-the-united-nations-sustainable-development-goals.aspx.

9   https://news.trendmicro.com/2023/05/10/what-is-dark-web/

Heightened concern regarding illegal activities on the dark web has been fuelled by the emergence of a wider 'criminal underground' – online communities for coordination of illicit activities. This underground naturally incorporates the dark web and sprawls across the broader ecosystem of the Internet, including increasingly encrypted communications platforms. The phenomenon known as 'crime-as-a-service' – a business model where criminals offer products or services to potential customers in exchange for a fee – plays an important role in this landscape. This model raises concerns particularly in the context of cyber threats – also known as 'cybercrime-as-a-service' – wherein all previously mentioned forms of cybercrime, along with other crime enablers such as digital fraud and bulletproof hosting, can be purchased as services. Cybercrime-as-a-service constitutes a significant paradigm shift in the world of cyber threats, effectively democratizing cybercrime by enabling individuals with varying degrees of technical expertise to access sophisticated capabilities and deploy cyber-attacks. Furthermore, these services, managed by individuals operating alone or by groups structured like legitimate businesses employing teams of developers, engineers, and technical support representatives, facilitate the scalability and commercialization of cybercrime as a whole, encouraging collaboration among cybercriminals from across the globe and expanding its geographical scope. This has amplified the challenges faced by investigators, by further obscuring the identities of individuals behind potential layers of other actors – adding a complexity that makes it increasingly difficult to clearly establish attribution for cyber-attacks, including understanding the motivations behind them.

Terrorism and Violent Extremism in the Cybercrime Underground

The anonymity of the dark web, coupled with the accessibility facilitated by cyber-crime-as-a-service, appeals not only to criminals but also to other actors with malicious intent, including terrorists as well as their supporters and sympathizers. The anonymity and privacy available in this cybercrime underworld provide an environment where they can engage in illicit actions with limited or little fear of detection or consequences.

Groups and individuals linked with terrorism and violent extremism have long been known to utilize the Internet and social media to plan recruit, train, exchange information, fundraise, acquire arms, transfer funds, and disseminate propaganda. In 2005, the United Nations Security Council recognized the importance for States to act cooperatively to prevent terrorists from exploiting sophisticated technology, communications, and resources to incite support for criminal acts,[10] a concern reiterated in 2014 in the context of addressing the increased use of communications technology for radicalizing individuals to terrorism, recruiting and inciting others to commit terrorist acts, including through the Internet, and financing and facilitating the travel and subsequent activities of foreign terrorist fighters.[11] The United Nations General Assembly, in the subsequent reviews of the United Nations Global Counter-Terrorism Strategy (A/RES/60/288) adopted in 2006, has similarly expressed deep concern over the use of the Internet and other information and communications technologies, including social media

---

10   Security Council resolution 1624 (2005).

11   Security Council resolution 2178 (2014).

platforms, for terrorist purposes, including the continued spread of terrorist content.[12] In recent years, terrorists have kept pace with innovation in terms of Internet and social media use, notably turning to live streaming their attacks on social media to amplify their impact. The first such case occurred during the 2019 attack on a mosque in Christchurch, New Zealand, and, more recently, in 2022 during the attack at the Buffalo Mall, United States of America.

While these actors have demonstrated a certain degree of proficiency with information and communications technologies (ICT) in various areas, it is widely reported that they lack the expertise to execute substantial cyber-attacks.[13] [14] [15] [16] [17] [18] The reasons for their limited involvement are often attributed to technical barriers to entry, coupled with lack of requisite funding and organizational efforts. Additionally, there is a belief that cyber-attacks may not provide the impactful spectacle of a physical act, such as violent attacks executed even with informal or rudimentary means. However, the ominous potential for terrorists and their supporters to leverage the opportunities presented in the dark web and capitalize on cybercrime-as-a-service is clear. Heightened ICT awareness and indications that these groups are recognizing the opportunity costs of cyber-attack strategies,[19] [20] combined with suggestions that kinetic (or physical) attacks may be becoming increasingly difficult due to the counter-strategies in place,[21] [22] raises substantial concerns.

Global Assessment of the Threat

Addressing a ministerial debate of the Security Council in 2019 on countering the threat of terrorism, United Nations Secretary-General António Guterres drew attention to the "dark side of the digital world" and the "new frontier" of crime-as-a-service. He flagged trends and developments in social media and the dark web to coordinate attacks, spread propaganda and recruit new followers.[23]

The General Assembly has also encouraged Member States to work together and with other relevant stakeholders, including academia, the private sector and civil society, to ensure that terrorists do not find safe haven online – particularly since the fourth review of the United Nations Global Counter-Terrorism Strategy in 2014 and its subsequent reviews, most recent-

---

12   Most recently, resolution 77/298 of the General Assembly (2023) for the eighth review of the Global Counter-Terrorism Strategy.

13   https://international-review.icrc.org/articles/counterterrorism-policies-in-the-middle-east-and-north-africa-916

14   https://press.un.org/en/2022/sc14995.doc.htm

15   https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209ws-study_en.pdf

16   https://www.london.gov.uk/sites/default/files/ctpn_preparedness_for_cyber-enabled_terrorism_report_single_pages.pdf

17   https://international-review.icrc.org/articles/counterterrorism-policies-in-the-middle-east-and-north-africa-916

18   https://press.un.org/en/2022/sc14995.doc.htm

19   https://www.steptoe.com/a/web/4586/231a.pdf

20   https://www.csis.org/analysis/global-terrorism-threat-assessment-2024

21   https://www.nato.int/cps/en/natohq/topics_156338.htm

22   https://www.gov.uk/government/publications/counter-terrorism-strategy-contest-2023/counter-terrorism-strategy-contest-2023-accessible

23   https://press.un.org/en/2019/sgsm19768.doc.htm

ly in its eighth review of the Strategy adopted in 2023. In doing so, it has stressed the need for international and multi-stakeholder cooperation to counter those who use ICT for terrorist purposes, while respecting human rights and fundamental freedoms and complying with international law and the purposes and principles of the Charter of the United Nations.[24] The Human Rights Council further elaborated on these issues in successive resolutions on the right to privacy in the digital age, calling upon States "to ensure that any measures taken to counter terrorism and violent extremism conducive to terrorism that interfere with the right to privacy are consistent with principles of legality, necessity and proportionality and comply with their obligations under international law."[25]

The Security Council has also been active with respect to the use of ICT for terrorist purposes, with fifteen resolutions being adopted over the years, addressing a variety of related topics such as digital evidence, public-private partnerships, crowdsourcing, and the utilization of emerging payment methods.[26] Notably, the Council has recognized the need for States to have the capacity to conduct open source and dark web investigations in the context of counter-terrorism. In October 2022, the Security Council's Counter-Terrorism Committee adopted the Delhi Declaration on countering the use of new and emerging technologies for terrorist purposes, which provides non-binding guidance on countering terrorist use of new and emerging technologies.[27] The Declaration serves as the Council's most recent acknowledgement of the adaptation of terrorists to, and the use of, new and emerging technologies, for terrorist purposes. It also highlights the concerns posed by online safe havens and underscores the need for Member States to take steps to counter the use of new and emerging technologies for terrorist purposes.

Despite the international community's ostensible recognition of the threat and the identified need for Member States' law enforcement and intelligence agencies to cooperate and develop their capabilities, there remains a gap in understanding whether and to what extent the nexus between terrorism and violent extremism, and cybercriminal elements on the dark web has manifested within the context of cybercrime-as-a-service for conducting cyber-attacks.

---

24   Resolution 68/276 of the General Assembly (2014) and subsequent reviews including most recently A/RES/77/298.

25   See for instance Resolution 54/21 of the Human Rights Council (2023.)

26   These include resolutions 1373 (2001), 1624 (2005), 1963 (2010), 2129 (2013), 2178 (2014), 2199 (2015), 2322 (2016), 2331 (2016), 2341 (2017), 2354 (2017), 2370 (2017), 2395 (2017), 2396 (2017), 2462 (2019), and 2617 (2021). https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_cted_factsheet_ict_march_2023.pdf

27   https://www.un.org/securitycouncil/ctc/news/delhi-declaration-countering-use-new-and-emerging-technologies-terrorist-purposes-now-available

This Report and Its Journey

Recognizing the significant knowledge gap around terrorism and violent extremism on the dark web and, specifically, how groups and individuals engaged in terrorism and violent extremism might leverage cybercrime-as-a-service to facilitate cyber-attacks, the United Nations Interregional Crime and Justice Research Institute (UNICRI) and the United Nations Counter-Terrorism Centre (UNCCT) of the United Nations Office of Counter-Terrorism (UNOCT) undertook an exploratory study to try to shed new light on this topic. This study, and the resulting report, consequently sought to clarify the existence of any nexus on the dark web between terrorism and violent extremism and cyber-criminality in the context of cybercrime-as-a-service. It also sought to identify emerging methodologies emanating from such a nexus and to ascertain how this impacts the overall assessment of the threat of cyber-attacks by groups and individuals engaged in terrorism and violent extremism. The report is intended to inform policymakers, law enforcement agencies, cybersecurity experts, and researchers engaged in counter-terrorism and cyber threats. Given the diverse nature of this target audience and levels of technical knowledge and understanding of the thematic, this report has adopted an introductory format.

Methodology

The findings presented in this report are based upon open-source desk-based research, including primary data collection from the dark web, encrypted communications channels, and the use of monitoring tools. This research also involved direct consultations with law enforcement agencies, cyber threat intelligence companies, and non-governmental organizations focused on terrorism and violent extremism. Additionally, data was collected through a survey issued to counter-terrorism and law enforcement agencies specializing in the dark web and/or cyber technologies mandated with countering terrorism.

Given the nature of the cybercrime underground and the inherent challenges in conducting research of this nature, this study has been exploratory in nature, rather than an attempt to provide a comprehensive or definitive analysis and overview of the terrorism, the dark web and cyber threats. Consequently, any information presented should be regarded as indicative of potential trends and developments. As outlined in the report, further research is required to develop a complete threat picture.

Challenges

The preparation of this report faced several challenges, with two standing out and meriting specific acknowledgment: definitions and data.

> *Definitional challenges* – The absence of internationally agreed definitions for terrorism and violent extremism presents significant challenges for any attempt to address the underlying research questions posed by this study. Variations in definitions can result in

contrasting perspectives and inconsistencies in how malicious actors are identified and categorized. This creates practical challenges when trying to establish a standardized framework for identifying, analysing, and assessing the actors in scope.

In the absence of a universally agreed definition for terrorism, and without prejudice to the diversity of terms used by Member States,[28] this report uses a description derived from United Nations Security Council resolution 1566 (2004). According to this resolution terrorism can be understood as "[...] criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism." Moreover, entities and individuals subject to the Security Council sanction regime pursuant to resolutions 1267 (1999), 1989 (2011), and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings, and entities, are considered terrorist.[29]

Similarly, there is also no internationally agreed definition of the term "violent extremism". The phenomenon is addressed at the United Nations in connection with terrorism, to the extent that both the General Assembly and the Security Council have underscored the need to prevent and counter violent extremism as and when conducive to terrorism. For technical purposes, this report considers that "violent extremism" is a diverse phenomenon, neither new nor exclusive to any region, nationality or system of belief. It encompasses a wider category of manifestations than terrorism. The report also recognizes the risk that a conflation of terrorism and violent extremism may lead to the justification of an overly broad application of counter-terrorism measures, potentially including forms of conduct that should not qualify as terrorist acts.[30]

Data Challenges – Attribution remains one of the foremost challenges in the field of cyber-security, largely stemming from the complex nature of cyber-attacks and the fact that digital evidence is easily manipulated or obfuscated. This often leads to ambiguity and uncertainty when it comes to understanding who is behind a cyber-attack. For this report, the additional difficulty of attributing the underlying motivations of terrorism and violent extremism to specific cyber-attackers has significantly hindered a definitive analysis of the dynamics of malicious actors on the dark web and within cybercrime-as-a-service. A multidisciplinary approach, integrating advanced forensic techniques, data analytics, international cooperation, and continual refinement of attribution methodologies would be required for a more comprehensive analysis. The necessary data and resources – such as seized media from dark web and cyber-attack investigations and blockchain analytical tools – exist but were unavailable due to the exploratory nature of this study. Pooling these data and resources would be essential for a more thorough analysis.

---

28   https://www.unodc.org/e4j/en/terrorism/module-4/key-issues/defining-terrorism.html#~:text=The%20implica-tions%20of%20the%20absence,even%20non%2Dcriminal)%20activities.

29   https://www.un.org/securitycouncil/content/un-sc-consolidated-list

30   Plan of Action to Prevent Violent Extremism, Report of the Secretary-General, A/70/674, 24 December 2015.

Stepping into the Cybercrime Underground

An essential first step in exploring the cybercrime underground is to establish a clear understanding of the distinct layers of the Internet. This section aims to lay foundational knowledge to clarify the nature of these layers, the origins of the dark web, how it functions and its role within the cybercrime underground. The evolution of the wider criminal underground will also be addressed, highlighting a need to consider the multiple layers of the Internet to ensure a holistic assessment of the threat. Recognizing the diverse target audience for this report, readers with a more advanced understanding may wish to advance to subsequent sections.

The Layers of the Internet

The first layer of the Internet is often referred to as the 'surface' or 'clear' or 'open' web and is the portion that is indexed and readily accessible to the public using regular search engines, such as Google, Bing or Yandex. While it is challenging to provide truly accurate figures for the size and dimensions of the Internet's layers, it is generally estimated that the surface web comprises no more than a few per cent. One assessment in the early 2000s put this figure at 5 to 10 per cent, and today, this is likely to be even smaller considering the overall growth of the Internet and the increase in unindexed data on the remaining layers.[31]

The next layer is what is referred to as the 'deep web' or 'deep internet'. This is the largest section of the Internet and is estimated to make up over 90 per cent of the total. While the term may lead some to believe this is a mysterious or possibly even criminal domain, this is not the case. Rather, it refers to the part of the Internet that is not indexed by traditional search engines like Google, Bing and Yandex and consists of content that requires specific credentials, permissions, or direct URLs to access. It encompasses a wide range of content, such as password-protected websites, online databases, private networks, academic and scientific resources, legal documents, and subscription-based services.[32]

---

31   https://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104).
32   https://www.kaspersky.com/resource-center/threats/deep-web

The final layer of the Internet is the darknet, otherwise known as overlay networks. This layer can only be accessed via specialist software that provides an enhanced level of anonymity through peer-to-peer connections using non-standard protocols and ports. It is within this layer that the so-called dark web exists, driven by the anonymity features that can provide a layer of protection for individuals engaged in illicit activities.

Some common examples of darknets are The Onion Router (Tor), The Invisible Internet Project (i2P), Freenet, Zeronet, and Lokinet. However, unless otherwise indicated, this report will focus on Tor, given its widespread recognition, large user base, and historical significance.[33] This focus does not imply the exclusion of other darknets, which offer their own unique features and merit their own analysis, however, concentrating on Tor for the purposes of this report allows for a more streamlined and accessible analysis of the largest dark web landscape.

While the terms dark web, darknets, and Tor are sometimes used interchangeably, it is important to emphasize a fundamental technical distinction between them. Darknets and Tor are essentially terms for the networks and software, and neither are inherently illegal. This kind of software and the accompanying networks are commonly and legitimately used by many for privacy purposes. On the other hand, the dark web necessarily implies illicit and illegal activities and is used to exclusively denote the nefarious websites and services hosted on these networks – predominantly dark web marketplaces, which are e-commerce platforms enabling anonymous transactions for various illicit goods and services, criminal forums where individuals discuss and exchange information related to illegal activities, and private websites hosting illegal products or services.

---

33   https://metrics.torproject.org

The Onion Router and the Dark Web

The dark web has its origins in the late 1990s as a project funded by the United States Defense Advanced Research Projects Agency (DARPA) with the goal of creating an anonymized and encrypted network for safeguarding sensitive communications. Some researchers involved in the project quickly recognized other significant potential uses, including supporting human rights and privacy activists. This recognition led to the establishment of the Tor network in 2006 – an open-source capability aimed at providing internet users with access to uncensored web content while preserving privacy.

The Tor platform utilizes a technique called "onion routing", a process in which data travelling the computer network is encapsulated in multiple layers of encryption – resembling the layers of an onion. The encrypted data passes through a series of decentralized servers called nodes (also known as "relays"), making it exceedingly difficult for unauthorized parties to trace the source or the destination of the message or access its content. This differs from traditional routing, which typically relies on single-layer encryption and fewer nodes and, in turn, has a lower level of user anonymity. The innovative approach of onion routing plays a central role in the widely used Tor Browser, which laid the technical foundation for the dark web and is now used by an estimated 4.6 million people each day.[34]

More specifically, the onion routing process involves layering access through a series of, typically, three nodes: entry (also known as "guard"), intermediate/middle, and exit. On the user's computer, a specialized programme encrypts requests for data with multiple keys, one for each node, before entering the network, and ensuring that each node can decrypt only its designated part. The entry node marks the user's arrival into the Tor network. The intermediate node, which is chosen randomly, decrypts the outer layer containing information about the data's forwarding path, but has no knowledge of the original data source or the final destination. Then the data is transmitted to the exit node, which plays a critical role, as it removes the last layer of encryption and forwards the data in its pure form to the desired address – meaning the message and destination address are visible to the server where the final website resides. By some, this is in fact considered a vulnerability in the whole process and may have been part of the motivation for the concerned community to explore alternative darknets and other decentralized networks such as I2P (Invisible Internet Project), Zeronet, Freenet, and Lokinet.[35]

---

34   For statistics on Tor, see: https://metrics.torproject.org/; https://www.statista.com/topics/11491/dark-web/#topicOverview; and https://www.statista.com/statistics/1414613/tor-average-daily-users-directly-leading/
35   https://changelly.com/blog/tor-network/

Tor random path to destination

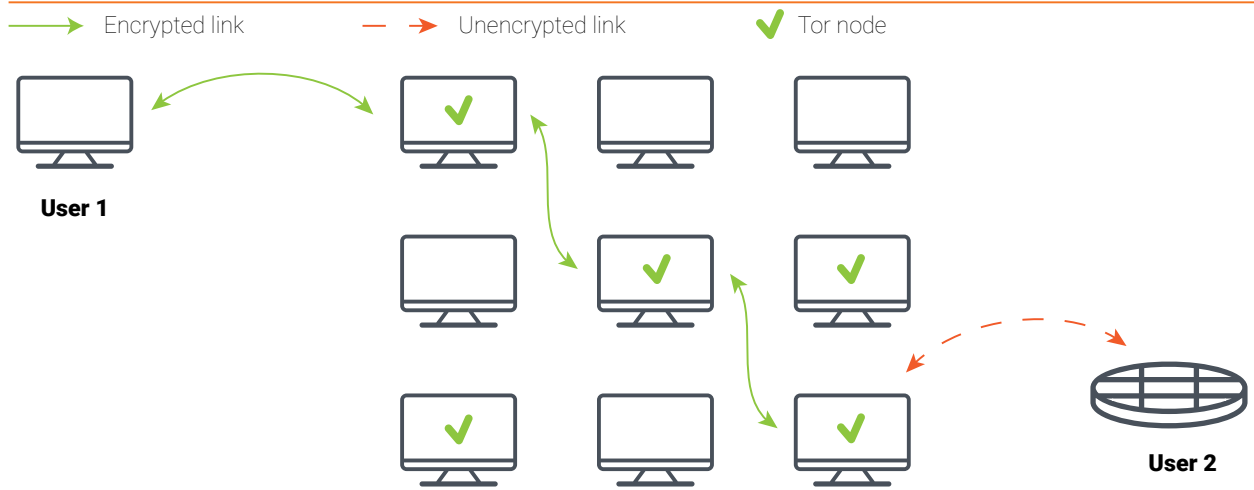Encrypted link →   Unencrypted link ─ ─→   ✔ Tor node

Image 1: How Tor Works

Another distinctive feature of the Tor network that has shaped the current landscape of the dark web is the ".onion" domain. This term refers to a special top-level domain suffix specifically designated for websites accessible only through the Tor network.[36] The use of .onion domains adds an additional layer of secure functionality, enabling the creation of websites within the network, often referred to as hidden sites. In addition to the technology, the security of these sites is further enhanced by unconventional naming structures and the need for users to know the URL beforehand.[37] It was this functionality that attracted the attention of the individual behind Silk Road – the infamous first market site created in 2011 on the dark web for anonymous trading in illegal goods and services. Following the takedown of Silk Road in 2013, similar sites have proliferated, giving rise to a complex illicit e-commerce on the dark web, and the subsequent evolution of crime- and cybercrime-as-a-service.[38]

Although there continues to be a wide array of marketplaces, forums and independent sites providing criminal products and services, the emergence of alternate darknets has added diversity and layers of complexity in the dark web landscape. Each of these networks employs encryption and decentralisation technologies that would appeal to malicious actors. This makes the advent of these darknets noteworthy, although there is limited information on the emergence of alternative darknets – among which I2P is most often cited – as viable contenders to Tor, which remains the backbone of the dark web. Furthermore, alternative darknets, when observed, often host replica "mirror" sites,[39] offering users additional options for access, rather than serving as direct replacements for Tor.

36   https://knowledge.digicert.com/general-information/onion-domains

37   https://www.expressvpn.com/blog/best-onion-sites-on-dark-web/#:~:text=Onion%20sites%20(aka%20Tor%20sites,-like%20.com%20or%20.net

38   https://www.crimeandjustice.org.uk/publications/cjm/article/inside-darknet-takedown-silk-road

39   A 'mirror' is a complete copy of a website or web page placed under a different URL but is identical in every other way https://www.techopedia.com/definition/4894/mirror-site

The Evolving Cybercrime Underground

Despite the historical and ongoing significance of Tor in shaping the dark web, there has been a noticeable shift in its popularity in recent years, necessitating a reconceptualization of our understanding of the dark web and the existence of a broader cybercrime underground when assessing the threat of cyber-attacks by terrorism and violent extremism.[40]

The growing culture around privacy has resulted in a surge of privacy-focused software, encompassing Virtual Private Networks (VPNs), privacy-orientated browsers, operating systems that prioritize anonymity, encrypted communication platforms, providers offering private email services, secure file storage solutions, and decentralized networks, including cryptocurrency (see Annex A). This proliferation has empowered individuals to remain anonymous without relying on Tor. These technologies can supply similar or improved anonymity, making those who know how to use them, including potentially malicious actors, less dependent on the functions provided by Tor. As a result, illicit activities have become more prominent across the wider digital domain beyond the dark web.

A key factor behind this is the growing use of encryption – the process of scrambling data to make it accessible only to authorized parties, involving converting human-readable plaintext into incomprehensible ciphertext.[41] The advent of encryption has given rise to various developments, most notably encrypted communication platforms – many of which are also popularly known and used as messaging apps. These platforms leverage encryption to maintain the privacy of communications, preventing unauthorized access to users' chats and calls. The most secure messaging apps implement end-to-end encryption, ensuring that only the sender and recipient can access the correspondence.[42] Using a secure messaging service with encryption not only protects users' data but also enhances overall privacy. Unencrypted messaging apps expose communications to the app company, advertisers, and hackers. In the event of a data breach, private information could be sold online or used for identity theft and other cybercrimes. Encryption is therefore central for the protection of a range of human rights, including the right to privacy, freedom of opinion and expression and interlinked rights.[43]

---

40   https://www.infosecurity-magazine.com/news/the-dark-web-goes-mobile/

41   https://www.cloudflare.com/en-gb/learning/ssl/what-is-encryption/

42   https://www.kaspersky.com/resource-center/preemptive-safety/messaging-app-security

43   See e.g. A/HRC/51/17; A/HRC/29/32.

However, in addition to its legitimate uses, cybercriminals seeking tools and services for maintaining anonymity exploit the offered encryption to secure their communications and reduce the risk of information breaches.[44]

Among cybercriminals, popular encryption communication platforms include Telegram, Signal, and Discord, with Telegram identified as a top medium of illicit cyber activity in 2023.[45] Cybercriminals increasingly prefer Telegram groups for anonymity and encrypted communication over in-forum messaging services. While Telegram dominates with 800 million users, other encrypted communication platforms are far from lagging behind. Signal experienced a 677% rise in downloads in January 2023,[46] and Discord, with almost 200 million active users and half a billion registered accounts in 2023, provides an open platform attracting cybercriminals for various malicious activities such as phishing, malware distribution, and social engineering. Whereas Telegram chiefly facilitates criminal communications, Discord's features have been reportedly used by malicious actors to execute diverse attacks within the app itself. Its file-sharing capabilities, voice and video chat options, and integrations with other apps offer an attack surface for malicious actors. Common attacks on Discord include phishing, where impersonation and artificial intelligence (AI) generated voices are employed, and malware distribution through file-sharing capabilities. Discord also shares many similarities with Telegram in terms of its use for criminal purposes, including the sale of illegal products and services and frauds.[47]

The rise to prominence of encrypted communication platforms underscores the advent of a broader cybercrime underground, with the dark web becoming just one tool in the toolkit of cybercriminals. Malicious actors are increasingly deviating from the exclusive and somewhat cumbersome dark web and exploring new avenues, such as encrypted communications platforms, and adopting new tactics and methodologies in line with what these avenues offer. While the present report focuses on the dark web in its classical sense, it is imperative to avoid compartmentalizing cyberspace – an error too often committed by governments and cybersecurity professionals – and instead understand and address the role of the dark web within the broader cybercrime underground.

Returning to the structure of the Internet, the 'Internet iceberg' is a metaphor that has long been used to explain its three distinct layers visually and conceptually: the surface web being the visible superficies, the deep web being the bulk of the submerged, and the dark web the very base of the iceberg. While this analogy is a helpful aid in understanding the layered and enormous nature of the Internet, it fails to capture the complexity of what is a fluid and evolving structure without static boundaries between layers.[48]

44   https://www.kaspersky.com/resource-center/preemptive-safety/messaging-app-security

45   https://www.darkreading.com/endpoint-security/exclu-shutdown-underscores-outsized-apps-messaging-apps-role-in-cybercrime

46   https://cybernews.com/security/cybercriminals-are-using-encrypted-chat-apps-as-illegal-marketplaces/

47   https://socradar.io/discord-the-new-playground-for-cybercriminals/

48   https://flashpoint.io/blog/internet-iceberg-redefine-the-web/

In this regard, a city may be a more appropriate way to conceptualize the layered and dynamic fabric of the Internet, providing a more nuanced representation of its diverse and interconnected components. In this metaphor, the bustling downtown, with its very visible network of streets, commercial units, and shining towers, represents the public and easily visible parts of the internet, like mainstream websites and social media platforms. Inside these buildings are the inner workings of business or residential properties, wherein people live their personal and private lives, which represent the private networks and databases that make up the deep web. The hidden corners and dark alleys of the city, which many inhabitants may not even know exist, reflect the discreet and sometimes dangerous corners of the dark web. The city analogy embraces the fluidity within buildings and between districts, providing a more relatable and nuanced representation of the ever-evolving and interconnected nature of the digital landscape throughout which the criminal underground exists.

Image 2: Illustration of the Internet as a city

Cybercrime-as-a-Service in the Cybercrime Underground

In the obscured recesses of the cybercrime underground, an ecosystem of illegal activities is burgeoning, centred around cybercriminal enterprises that offer cybercrime-as-a-service. Estimated to generate annual revenue exceeding $1.6 billion USD,[49] cybercrime-as-a-service encompasses a wide range of traditional crime-enabling activities seamlessly adapted to the digital realm. For example, fraud services flourish with the provision of compromised credit cards to fund further cybercriminal endeavours. Identity services provide stolen personal data, like passports useful for impersonation and bypassing "Know-Your-Customer" checks when creating cryptocurrency wallets or exchanging fiat currency. The expansive ecosystem also fuels sophisticated technical elements of cybercrime, including hacking-for-hire for network intrusion, the development and distribution of malware (including ransomware kits), stressor tools for distributed denial of service (DDoS) attacks, online social engineering capabilities, phishing attacks, exploits, credential stuffing and the sale of stolen personal data. This concept of cybercrime-as-a-service has reshaped the cybercrime landscape, enabling malicious actors to access a variety of tools, resources, and expertise essential for executing cyber-attacks with heightened ease and efficiency. This not only lowers the entry barriers for aspiring criminals but also facilitates collaboration among specialized individuals or groups, amplifying the scale and impact of cyber-attacks while transferring risk and avoiding detection.

The examples provided below offer only a glimpse into the landscape of cybercrime-as-a-service and are exclusively for illustrative purposes. It is important to highlight, cybercrime is a dynamic and multifaceted concept that involves various types of malicious actors, each contributing distinct roles within an ever-expanding cyber threat landscape. Consequently, the products and services accessible for purchase or hire on the dark web are significantly shaped by the evolving needs and capabilities of cybercriminals, advancements in technology, and the latest developments in cybersecurity vulnerabilities and countermeasures. The commercialization of other criminal elements is therefore an ongoing trend, with new services continually emerging.

Distributed Denial of Service (DDoS)-as-a-Service

DDoS-as-a-Service is where malicious actors lease their available capabilities to those seeking to launch distributed denial of service (DDoS) attacks on their targets. A DDoS attack occurs when malicious actors inundate a target server with numerous requests to overwhelm it and disrupt its responsiveness to legitimate requests. This service spares criminal customers from the necessity of building their own extensive botnets – large networks of compromised computers typically established through compromised Internet of Things (IoT) devices – or coordinating the attack themselves by attacking virtual private servers (VPS) using known exploits or leaked application programming interface (API) credentials.

A significant illustration of the impact of DDoS attacks is evident in the case of Microsoft. The company confirmed that the outages experienced by Azure, Outlook, and OneDrive web

---

49   https://fieldeffect.com/blog/cybercrime-as-a-service

portals in 2023 were a result of Layer 7 DDoS attacks against its services.[50] In a Layer 7 DDoS attack, malicious actors focus on the application level, inundating services with a massive volume of requests, causing the services to become unresponsive as they struggle to process the overwhelming load. Each DDoS method works by overpowering a web service, utilizing all available connections, rendering them incapable of accepting new requests.[51]

The aftermath of an attack of such magnitude could potentially yield numerous adverse effects. While Microsoft affirmed that there were no breaches of users' data following the Layer 7 DDoS attack, this outcome is not guaranteed in all cases, given the potential indirect impact on overall system integrity. Microsoft recognized this risk and advised users to implement specific mitigation measures to enhance protection against potential subsequent attacks.[52]

Despite law enforcement interventions over the past two decades, DDoS-as-a-Service has endured and continues to be employed by malicious actors with diverse motivations. The evolving trend exhibits no signs of deceleration, with cybersecurity companies such as Cloud-Flare identifying a staggering 532% increase in DDoS attacks in just the second quarter of 2023 alone.[53] Furthermore, there are emerging indications that malicious actors are integrating DDoS with other forms of cyber-attack, such as ransomware.[54]

Image 3: How DDoS Attacks Work

50   https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-azure-outlook-outages-caused-by-ddos-at-tacks/
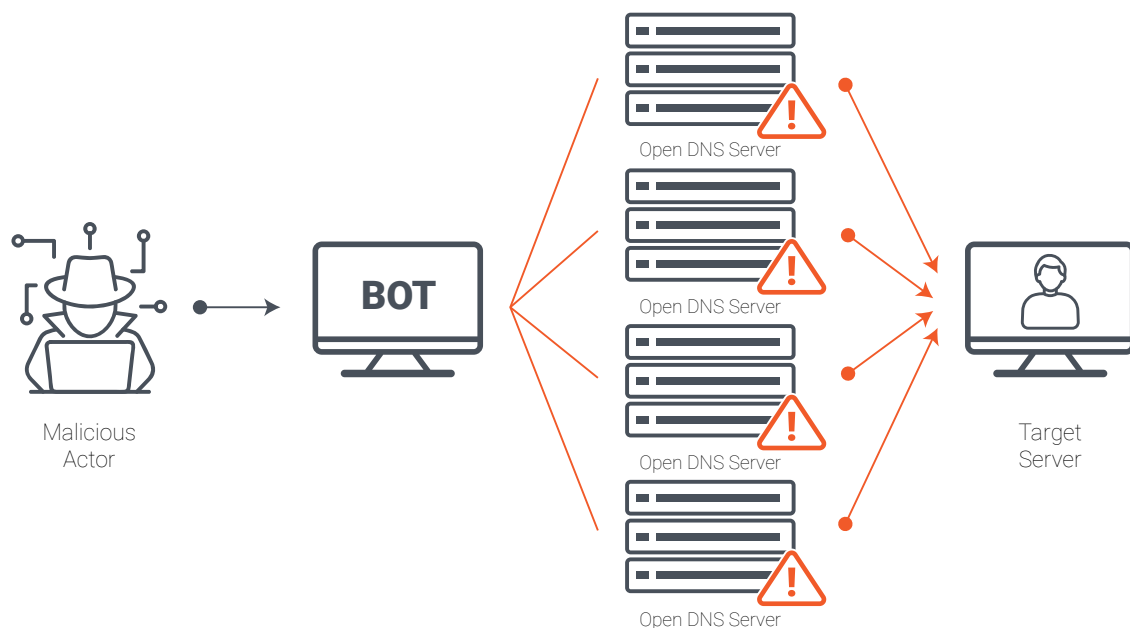51   https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-azure-outlook-outages-caused-by-ddos-at-tacks/
52   https://www.techtarget.com/searchsecurity/news/366542236/Microsoft-DDoS-attacks-caused-M365-Azure-disrup-tions
53   https://blog.cloudflare.com/ddos-threat-report-2023-q2/
54   https://www.slcyber.io/attack-for-hire-services-the-evolution-of-ddos/

Ransomware-as-a-Service (RaaS)

Ransomware-as-a-Service remains a highly prevalent cyber threat, with notable instances of attacks on critical infrastructure, including healthcare and energy providers, where malicious actors aim to undermine government services and impact communities. It is an essential cybercrime-as-a-service offer, which has played a pivotal role in the expansion of ransomware attacks through affiliate programmes. The business model revolves around the ransomware developers creating and administering online platforms that approved affiliates use to access and deploy the ransomware and share exfiltrated data. In return, the developers receive a percentage of the ransomware payments generated by the affiliates. This dynamic has contributed to the proliferation of extortion groups – a trend that appears set to continue.[55] [56]
When creating affiliate programmes, developers may relinquish some control over the use of their malware. In doing so, terms and conditions will be agreed with affiliates to include usage restrictions, for example agreements not to target certain types of institutions. This is a common practice on the dark web; however, adherence to these restrictions is not always guaranteed. Furthermore, the ability of developers and affiliates to disassociate from each other adds a layer of complexity to attribution, posing additional challenges for law enforcement investigations.[57]

A highly significant illustration of the far-reaching consequences of ransomware attacks is the 2021 incident involving the Colonial Pipeline. This cyber-attack brought the pipeline offline, causing widespread panic in the United States and gaining global attention. The attack brought Colonial Pipeline's operations to a standstill for approximately five days, resulting in localized shortages of gasoline, diesel fuel, and jet fuel and prompting panic-buying due to the imminent depletion of gas supplies.[58] The attack also had broader societal and financial ramifications, prompting Colonial Pipeline to proactively shut down its operational technology systems to prevent further infection. Eventually, the company paid the hackers $4.4 USD million[59] in cryptocurrency to restore its operating systems. Despite receiving the decryption key, restarting the pipeline required days of effort.

55   https://www.coveware.com/blog/2022/1/26/ransomware-as-a-service-innovation-curve
56   https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight%20Report%20-%20Cyber-attacks%20 the%20apex%20of%20crime-as-a-service.pdf
57   https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight%20Report%20-%20Cyber-attacks%20 the%20apex%20of%20crime-as-a-service.pdf
58   https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colo- nial-pipeline-ransomware-attack/#~:text=The%20attack%20shut%20down%20Colonial.feared%20gas%20would%20r- un%20out.
59   https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636
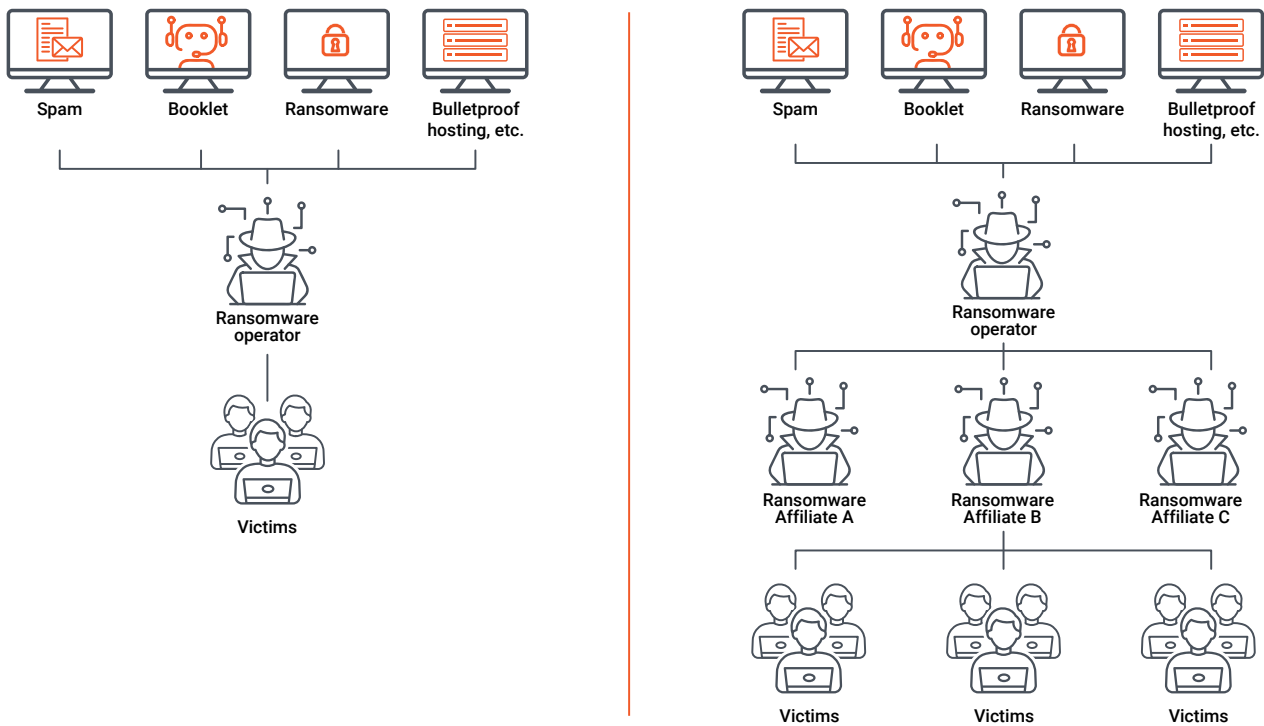
Image 4: Ransomware vs. RaaS

Access-as-a-Service

Access-as-a-service (AaaS) is a growing extension of the cybercrime-as-a-service model, where malicious actors offer a point of access to business networks as a product. Perpetrators, known as Initial Access Brokers (IAB), operate opportunistically, capitalizing on identified vulnerabilities to generate profit. Alternatively, some act as dedicated sellers, operating their ventures with structured marketing strategies and online vendor shops. This service does not include continuous access provision, instead it is a product typically comprised of a set of credentials along with a VPN server for connection. Serving as a facilitator, this function can yield adverse effects across various sectors and serves as a valuable enabler for malicious actors looking to execute subsequent cyber-attacks, regardless of their underlying motivations.

The rise of AaaS has further amplified the threat of ransomware attacks since 2020.[60] While ransomware visibly dominates the impact of such breaches, the silent facilitators – those discreetly breaching and selling access to other malicious actors – play a critical role in enabling these attacks.[61] This dynamic implies a positive correlation, suggesting that as RaaS and ransomware attacks continue to increase, AaaS is likely to follow suit.

---

60   https://www.trendmicro.com/vinfo/gb/security/news/cybercrime-and-digital-threats/investigating-the-emerging-ac-
        cess-as-a-service-market
61   https://www.trendmicro.com/vinfo/gb/security/news/cybercrime-and-digital-threats/investigating-the-emerging-ac-
        cess-as-a-service-market

Image 5: How Access-as-Service Works

Image 6: How Selling Access Takes Place

Stolen Data-as-a-Service (SDaaS)

A common thread linking the aforementioned malicious activities is the acquisition and exploitation of stolen data, which serves as a prized illicit commodity, representing a virtual gol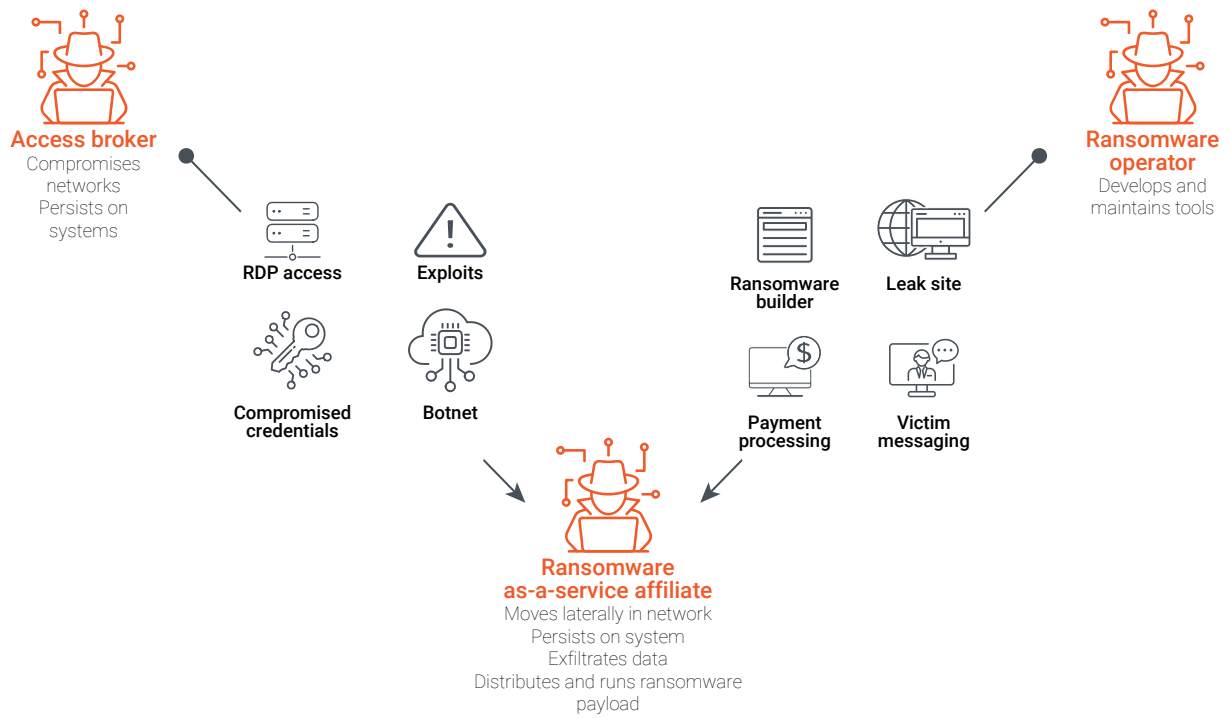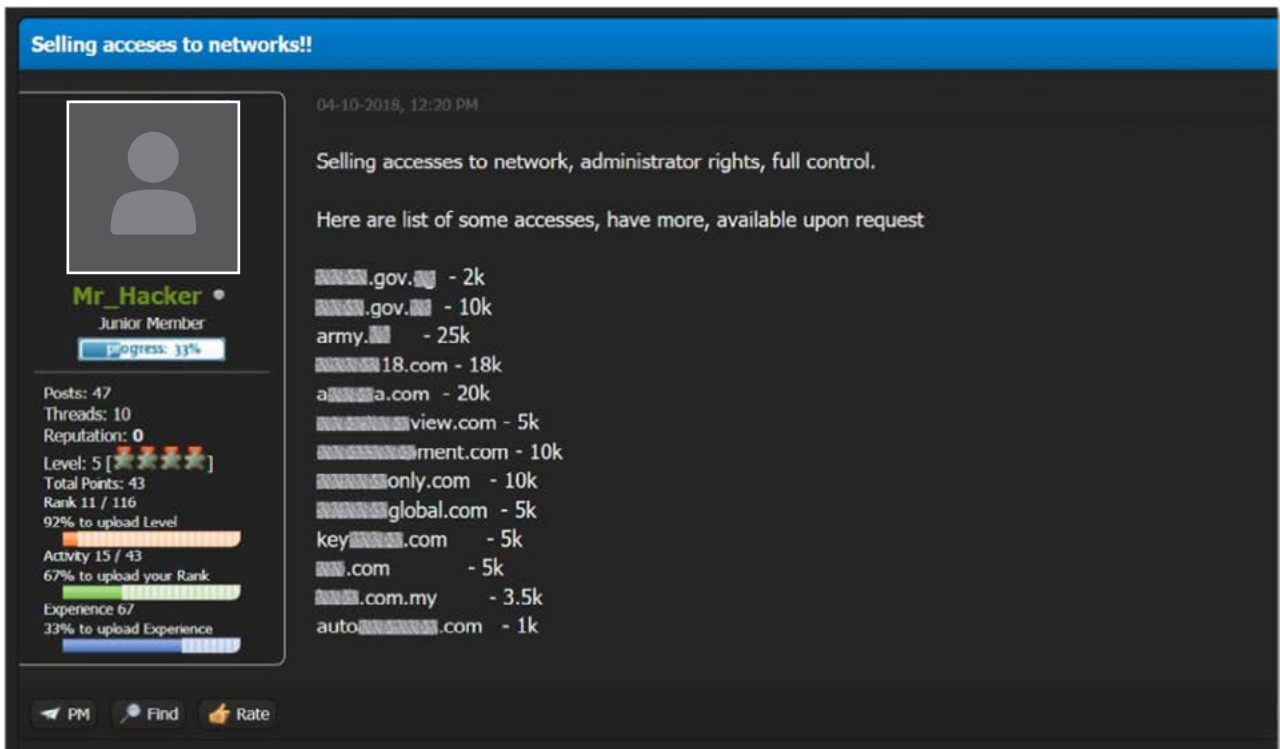dmine for further potential threats. As a result, Stolen Data-as-a-Service (SDaaS) emerges as a by-product of cyber-attacks and key enabler for subsequent malicious activities. Routinely exchanged across the cybercrime underground, this pilfered data becomes a highly profitable and sought-after product that cybersecurity measures strive to protect against.[62]

Several notable examples of the largest data breaches in history include Yahoo (2013) with 3 billion records, First American Corporation (2019) with 885 million records, and the Indian Council for Medical Research (2023) with 815 million records. In 2023, it is estimated that a staggering 8,214,886,660 records were breached globally,[63] a figure expected to increase in 2024 in tandem with the overall predicted growth of cybercrime. These attacks can result in diverse social and financial impacts, particularly when considering that leaking sensitive government information can have political, financial and privacy-related implications. Moreover, selling the data on the dark web not only generates revenue but also magnifies the impact of the attack by placing sensitive information in the hands of other malicious actors.[64]

SDaaS has emerged as a formidable adversary for cybersecurity companies. It constitutes a highly profitable business, with 93% of its providers primarily driven by financial motives.[65] Given the financial reward, SDaaS will persist as a significant threat to cybersecurity.

Personal data stored on servers — **Hackers break in and steal personal data** — *(Where applicable)* **Data given to broker to sell on social networks.** — **Buyer purchases data to commit identify fraud or for use in further cyber attacks and/or other crime**
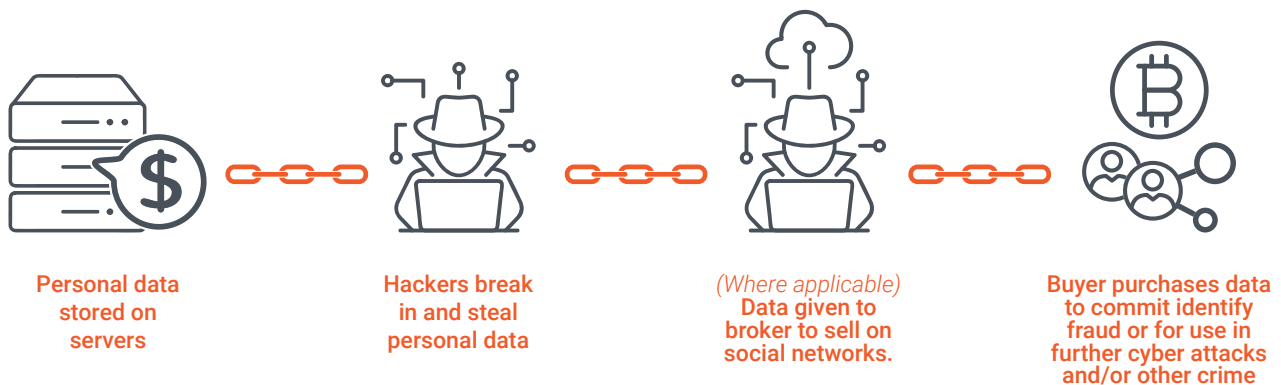
Image 7: The Stolen Data Supply Chain

62   https://theconversation.com/darknet-markets-generate-millions-in-revenue-selling-stolen-personal-data-supply-chain-study-finds-193506

63   https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023#~:text=See%20the%20full%20list%20of%20data%20breaches%20for%20September%202023&text=September%20saw%20the%20biggest%20data,misconfigured%20Elasticsearch%20and%20Kibana%20interface.

64   https://socradar.io/dark-web-profile-bjorka/

65   https://terranovasecurity.com/blog/cyber-security-statistics/

Other Services

There are numerous other capabilities within the realm of cybercrime-as-a-service, and every facet of the cybercrime ecosystem is being commercialized. For example, "bulletproof" hosting services and some VPN services cater to cybercriminals, offering covert hideouts for malicious activity and are designed to withstand abuse complaints and law enforcement takedown requests.

Financial services also play a crucial role in the execution of cyber-attacks, with an explosion of services, including cryptocurrencies, unregistered exchanges, cross-chain bridging and mixing services becoming available.[66.] These are widely available on the dark web, and are actively utilized by a myriad of malicious actors.

Specializing in different facets of cybercrime as-a-service, groups collectively contribute to the rapidly growing complexity and sophistication of illegal operations in the digital domain. The collaborative and dynamic nature of this model has created an environment where cyber-criminals can collaborate to access the range of tools and support needed to execute a wide variety of attacks. This environment poses a substantial and constantly evolving challenge to global cybersecurity efforts.

---

66   Cryptocurrency Mixer: a technical service that combines the cryptocurrencies of multiple users to obfuscate the
        origins and owners of the funds.

Terrorism, Violent Extremism and Cybercrime-as-a-Service on the Dark Web

Cyber-Attack Capabilities and Intentions

The aspirations of terrorist groups and individuals to develop cyber strategies is evident, with designated terrorist groups involvement in cyber-attacks seen as far back as Al-Qaida in the late 1990s.[67] Notably, in more recent times, the group released a widely reported video in 2011 declaring an "electronic jihad" against the United States and calling upon its followers to launch cyber-attacks against critical infrastructure in the United States.[68] Da'esh has mirrored these aspirations, with various calls throughout its rise to prominence urging supporters to hack the websites of "Western" governments.[69] In December 2023, they made a specific call for attacks on sites associated with the Jewish community through the dark web publication "Voice of Khurusan."[70] "The Islamic State Hacking Division," the "Caliphate Cyber Army," and the "United Cyber Caliphate" – hacking groups associated with Da'esh – have been at the forefront of the group's cyber activities and played a key role in its extensive use of social media.[71]

Notwithstanding what can be described as a pattern of purposeful engagement in cyber activities and declared interest in offensive activities in this space,[72] the cyber-attack capabilities of these groups remain ostensibly limited, with little more than low-level hacks, defacement of official sites, and doxing (publicly releasing an individual's personally identifiable information) taking place. Various studies have speculated that the reasons for this limitation revolve around the technical barriers to entry, coupled with the need for requisite funding and organizational efforts, and a belief that cyber-attacks may be less impactful in terms of spectacle than a physical act.[73] [74] However, the threat of significant cyber-attacks by terrorist actors moving forward should not be disregarded. Da'esh has, for instance, actively sought to recruit cyber-skilled individuals into their ranks to aid in their efforts,[75] and instances have been reported where, in the absence of internal expertise, terrorist groups and individuals have sought to leverage the expertise. This was most prominently seen in the case of Ardit Ferizi, or "Th3Dir3ctorY" – a hacker who, in 2015, gained system administrator-level access to servers in the United States and extracted personally identifiable information of approxi-

---

67   https://www.unodc.org/documents/e4j/18-04932_CT_Mod_01_ebook_FINALpdf.pdf

68   https://cvir.st-andrews.ac.uk/articles/10.15664/jtr.1183

69   https://www.politico.com/story/2015/12/isil-terrorism-cyber-attacks-217179

70   https://www.adl.org/resources/blog/islamic-state-al-qaeda-call-violence-against-jewish-communities-following-october-7

71   Each of these groups is considered associated and affiliated with Da'esh, although the level of formal engagement with Da'esh remains unclear. List of groups considered associated with Da'esh: https://scsanctions.un.org/uw-9bqen-al-qaida.html#alqaedaent

72   See Tech Against Terror – State of Play 2022 Report: https://www.techagainstterrorism.org/hubfs/FINAL-State-of-Play-2022-TAT.pdf ..

73   https://www.usip.org/sites/default/files/sr119.pdf

74   https://www.usip.org/sites/default/files/sr119.pdf

75   https://home.treasury.gov/news/press-releases/jy2056

mately 1,300 United States military and government personnel. He subsequently made contact with Da'esh members via Twitter and Skype and handed over this information to the "Islamic State Hacking Division," which subsequently published the data.[76]

Over the past decade, terrorist groups have demonstrated increasingly enhanced technical awareness. Some groups boast dedicated technical teams that develop and advocate for innovative methods to evade law enforcement.[77] This is consistent with the enhanced use of the dark web and technology across the cybercrime underground. For instance, Da'esh and Al-Qaida have both adopted Rocket-chat, an open-source decentralized software that enables users to establish their own server instances[78]. This strategic move has allowed these groups to create even more secure and private communication channels.[79] Their sophistication also extends to further evasive capabilities designed to thwart security services. For example, in 2022, the pro-Da'esh cyber security capability "Electronic Horizon Foundation" released a short instructional video via their dark website and social media channels about "Locker," a smartphone security capability that would automatically erase all data after several unsuccessful attempts to unlock the device.[80] They have also exhibited an increased technical understanding of blockchain technology and cryptocurrency, which are heavily featured as services on the dark web. Bitcoin was the first cryptocurrency seen to be used by these groups for crowdfunding campaigns and it remains commonplace for broader terrorist financing and money laundering.[81] [82] Recent trends also indicate a further shift toward capabilities perceived to be less susceptible to crypto-tracing, such as the more privacy-centric Monero, which is primarily used for donation campaigns, decentralized finance (DeFi), mixing services and cross-bridging to alternative blockchains, with the widespread use of TRON and Tether stablecoin (USDT) being as a prominent trend reported by experts.[83]

There is also some evidence of the cyber capabilities and intentions of some individuals inspired by terrorism on the basis of xenophobia, racism, and other forms of intolerance, or in the name of religion or belief (XRIRB).[84] In one notable case, a hacker, thought to be motivated by COVID-19 conspiracy theories, allegedly distributed approximately 25,000 e-mail credentials from the Gates Foundation, the World Health Organization (WHO), and the United States Center for Disease Control and Prevention (CDC) on a neo-Nazi Telegram channel.[85]

---

76   https://www.justice.gov/opa/pr/isil-linked-kosovo-hacker-sentenced-20-years-prison
77   https://home.treasury.gov/news/press-releases/jy2056
78   https://flashpoint.io/blog/rocket-chat-remains-resilient-platform-for-jihadists/
79   https://flashpoint.io/blog/rocket-chat-remains-resilient-platform-for-jihadists/
80   https://www.memri.org/cjlab/pro-isis-outlet-releases-video-guide-installing-using-locker-phone-data-erasing-app
81   https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf
82   https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf
83   https://www.trmlabs.com/post/terrorist-financing-six-crypto-related-trends-to-watch-in-2023
84   https://isc.independent.gov.uk/wp-content/uploads/2022/07/E02710035-HCP-Extreme-Right-Wing-Terrorism_Accessible.pdf
85   https://www.cyberdefensemagazine.com/covid-19-neo-nazis-spread-a-list-of-credentials-for-gates-foundation-nih-and-who-employees/

In recent years, there has also been a notable rise in cybercrime by malicious actors purportedly motivated by considerations other than financial.[86] Such individuals and groups, or 'collectives', are often branded as 'hacktivists' and seek to utilize cyber-attacks to advance their political, religious, or social beliefs, targeting entities perceived as adversaries or aligned with opposing belief systems. The technical capabilities of these malicious actors can vary but their fluidity enables calls to action for cybercriminals across the cyber skillset in support of diverse causes. Leading examples of these types of groups would be Anonymous – the decentralized hacktivist collective – as well as GhostSec, ThreatSec, SiegedSec, Killnet, and Anonymous Sudan, to name but a few. Notably, these groups claim to have targeted critical infrastructure, including hospitals and utility systems, and express the explicit intent to maximize societal impact, inflicting extensive damage, with clear disregard for harm to innocent individuals.[87] Interestingly however, some of these groups have since taken steps to distance themselves from this initially evident disregard for harm. In October 2023, the International Committee of the Red Cross (ICRC) issued a set of guidelines that outlines rules of engagement for civilian hackers involved in conflict grounded in international humanitarian law,[88] which has been welcomed by some hacktivist groups. Notably, this includes Killnet, which pledged to comply with the guidance.[89] Despite such developments, however, this general phenomenon in the threat actor landscape weighs heavily in light of the growing scale of cyber-attacks and blurs attempts to distinguish between acts that are perpetrated by criminals or extremists in nature.

It is important to emphasize that criminality, hacktivism, terrorism and violent extremism should not be conflated, all the more so in the absence of internationally agreed definitions and given the concern that the definitions in many national jurisdictions are either lacking or not sufficiently clear and precise to comply with international human rights law, including guaranteeing the right to freedom of expression. At the same time, there must be an effective and proportionate law enforcement and criminal justice response to hold criminal actors appropriately accountable for cyber-attacks, uphold the rights of victims, and deter further attacks.

---

86   https://www.recordedfuture.com/threat-intelligence-101/threat-actors/cybercriminals
87   https://blogs.blackberry.com/en/2024/03/critical-infrastructure-cyberattacks-2024
88   https://blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obligations-states-restrain-them/.
89   https://quointelligence.eu/2023/11/red-cross-rules-of-engagement-for-hacktivists/

A Summary of Findings and Dynamics Observed

In delving into the complex interplay between terrorists and cybercriminals and their methodologies, the research underscores the importance of several elements of the dark web and cybercrime-as-a-service as pivotal facilitators of cybercrime, providing accessible avenues for malicious actors to enhance their capabilities and engage in cyber-attacks. The anonymity and convenience offered by the dark web, alongside its various underground markets and forums, provide a secure and enabling environment for cybercrime-related activities. Moreover, cybercrime-as-a-service not only equips these malicious actors with technical capabilities, lowering the barrier of entry to cyber-attack execution, but also encompasses auxiliary services like money laundering, encryption, and secure communication channels. The findings also emphasize the need to understand the implications of the dark web and cybercrime-as-a-service within the broader cybercrime underground to fully comprehend the nature of the threat posed by terrorism and violent extremism when it comes to cyber-attacks.

Recognizing the challenges of defining terrorism and violent extremism and attributing specific cyber-attack activities to the dark web and cybercrime-as-a-service, this section will consider threat actors more broadly – specifically individuals or groups who utilize cyber-attacks to advance their political, religious, or social beliefs, targeting entities perceived as adversaries or aligned with opposing belief systems. Such threat actors could be said to be motivated more by a belief system than purely by financial considerations. By examining their tactics, techniques, and procedures employed, reasonable inferences can be drawn as to what may also be plausible or possible in the specific context of terrorism and violent extremism. It is hoped that this can help inform effective counter-strategies by policymakers, law enforcement agencies, cybersecurity experts, and researchers engaged in counter-terrorism and cyber threats.

Dark Web Marketplaces

Multiple sources have highlighted the link between threat actors and dark web marketplaces. Links to terrorism specifically have been observed; for example, the weapons used in the attacks in Paris, France, in 2015 and in Munich, Germany, in 2016, were allegedly acquired from vendors operating on the dark web.[90] It is also widely reported that fraud enablers, such as stolen credit cards and stolen passports, have been acquired by terrorist groups on dark web marketplaces.[91] While this supports a clear indication that dark web marketplaces are being used by terrorist groups and individuals, there is insufficient information to establish the true nature of the interactions and to what extent these can be attributed to cyber-attacks.[92] However, an absence of sufficient information does not imply they do not exist. Rather, a confirmed association cannot be made due to limitations in available data to clarify what the interactions entailed. Nonetheless, considering the confirmed use of dark web marketplaces by these malicious actors, the cyber-attack calls to action observed, and the enabling cybercrime capabilities the dark web marketplaces are known to provide,[93] it can be inferred that these do serve as enablers exploited by terrorists and their sympathizers to execute cyber-attack strategies, especially when a fraud or money laundering component is involved.

Independent Dark Web Domains (.onion)

Threat actors have been observed creating their own concealed services on the dark web using independent domains (.onion).[94] The purpose of these is wide-ranging, with terrorist groups and hate groups in general observed using them for news and propaganda, examples being the official publications of the Afghanistan-based Islamic State in Khorasan Province (ISKP) and the neo-Nazi website 'The Daily Stormer'. Threat actors have also been observed using these domains to host blogs providing additional information about their activities and for storing stolen data.[95] [96]

Unlike dark web marketplaces, which tend to publish URLs on dark web information sites and forums, threat actors commonly publish their dark web URLs on the surface web, deep web, encrypted communication platforms like Telegram, or on specialist dark web cybercrime forums. Additionally, the content on these domains is often not exclusive to the dark web, and replicas of the information can often be found elsewhere across the criminal underground.

It is surmised that the reason for the use of independent dark web domains may be to provide an alternative option for users who prefer the protections offered by darknets. The utilisation of these sites is also believed to ensure sustained access, as it proves more challenging for platform providers and law enforcement to take the information offline.[97]

---

90   https://www.wsj.com/articles/before-the-shootings-munich-gunman-visited-the-dark-web-1469558210
91   https://www.elliptic.co/blog/how-terrorist-organizations-are-exploiting-crypto-to-raise-funds-and-evade-detection
92   https://www.rand.org/pubs/commentary/2018/01/bitcoin-and-the-dark-web-the-new-terrorist-threat.html
93   https://www.elliptic.co/blog/how-terrorist-organizations-are-exploiting-crypto-to-raise-funds-and-evade-detection
94   https://www.tandfonline.com/doi/pdf/10.1080/19434472.2022.2164326
95   https://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf
96   https://www.researchgate.net/publication/221400240_Dark_Web_Exploring_and_Mining_the_Dark_Side_of_the_Web
97   https://dailystormer.info/

Cybercrime Forums

Similarly to dark web marketplaces, there is an array of criminal forums nestled within the dark web, providing a space for various threat actors to share information, trade in illegal products and services, and connect with like-minded individuals. Similarly to independent domains, these platforms are often mirrored on both the deep and dark web, serving as convenient digital meeting places for threat actors throughout the criminal underworld.[98]

Unlike dark web marketplaces, which are oriented toward the trade in various illicit goods, criminal forums typically exhibit a more specialized focus. This is particularly evident in the realm of cybercrime, exemplified by cyber-focused forums like Breachforums, XSS.in, and Exploit.in.[99] These forums provide for activities such as technical knowledge sharing, networking, accessing hacking tutorials, selling compromised credit cards, breached data, and cybercrime products and services.

Cybercrime forums are widely used by malicious actors driven by both financial and other motivations.[100] Their popularity can be attributed to the access they provide in keeping up with the ongoing evolution of cyber-attack capabilities, and the role they play in enhancing technical proficiency.[101] Forums can also serve as platforms for transactions, and some administrators, like those from Blackforums – a popular option for non-financially motivated threat actors – have also been alleged to run their own services, such as Telegram marketplaces and bulletproof hosting services. Furthermore, criminal forums publicly providing personally identifiable information enable private messaging and more restricted communication channels where detailed discussions and sensitive attack planning can take place. However, akin to dark web marketplaces, the lack of visibility into these restricted layers makes it challenging to draw substantive inferences, albeit the wider use of cybercrime forums by threat actors with motivations other than financial is clear.

Encryption and Privacy-Focused Capabilities

Threat actors are becoming increasingly technically aware and security-conscious online. The promotion of VPNs is actively encouraged for threat actors using the darknets, while others appear confident in their ability to maintain anonymity without relying on Tor. Consequently, threat actors have become more active across encrypted communications platforms, with Telegram portrayed as a rapidly emerging "new dark web" for cyber-attacks in the broader cybercrime underground.[102] However, it is observed that particularly terrorist groups appear willing to communicate openly on Telegram's public channels. While this openness aids in generating interest in their cause and inciting further activity, it also reveals a lesser concern about detection and the need for darknets to mask their activity.

98   https://techjury.net/blog/dark-web-forums-to-follow-to-stay-ahead-of-cyber-threats/
99   https://webz.io/dwp/the-top-dark-web-forums-in-2023/
100   https://www.slcyber.io/2023-in-review-hacking-forums-and-dark-web-marketplaces/
101   https://www.slcyber.io/2023-in-review-hacking-forums-and-dark-web-marketplaces/
102   https://www.ft.com/content/cc3e3854-5f76-4422-a970-9010c3bc732b

In contrast, research also highlights discussions within the non-financially motivated threat actor circles regarding other encryption Tor-based capabilities, such as Decentra, a Tor-based bot manager for illicit market activities, as well as the promotion of GetTor, a Tor browser, via Telegram channels. Likewise, the prevalence of anonymous Tor-based mail servers is evident, and in the context of this report, Mail2Tor is worthy of note. Although not dark web, in a similar vein, other privacy-focused platforms, such as anonymous file-sharing services or mail servers, play crucial roles in the methods employed by some threat actors. Numerous reports underscore the widespread use of anonymous file-sharing to communicate and share information. For instance, threat actors involved in attacks on critical infrastructure were identified as utilizing a variety of platforms, such as Anonymfile, Mega.nz, and Catbox to share information. Furthermore, Discord's file-sharing features have been reported as providing an attack surface in and of itself, allowing threat actors to execute attacks using infected files.[103] Research has also confirmed instances of threat actors utilizing commonly available cloud services like Dropbox, Google Drive, Microsoft OneDrive, and Amazon Cloud Drive.[104]

Cryptocurrencies

Cryptocurrencies have become a fundamental element of cybercrime and serve as the financial backbone for cybercrime-as-a-service. The decentralized networks and perceived anonymity make them the preferred method for both financially and non-financially motivated threat actors. They facilitate a range of activities, from the purchase and sale of cyber-attack products and services to enabling other forms of terrorist financing and money laundering. Furthermore, cryptocurrency itself can be an end-goal commodity in cyber-attacks carried out for the purpose of terrorist funding.

The cryptocurrency ecosystem provides various obfuscation opportunities, including multiple blockchain and token options. Services include crypto ATMs, coin-swapping, mixing services, DeFi, and cross-chain bridges, many of which have been observed in use by groups such as Da'esh, Al-Qaida, and violent right-wing groups involved in the violence at the United States Congress on 6 January 2021.

---

103   https://intel471.com/blog/how-discord-is-abused-for-cybercrime
104   https://www.euronews.com/2018/09/04/terrorists-are-misusing-cloud-services-to-incite-violence-the-eu-must-do-more-to-stop-them

Furthermore, while the cryptocurrency ecosystem is broad and spans the digital space, a surge in crypto-as-a-service has been observed across the dark web, particularly coin-swapping, cross-chain bridges, and mixing services. There is a lack of comprehensive data to establish the extent to which threat actors are using these particular services and whether this is for the purposes of cyber-attacks. Nonetheless, existing research does suggest a discernible pattern. Reports confirm the expansion of terrorist financing initiatives to encompass more than 30 different cryptocurrencies, many of which are utilized in fundraising endeavours.[105] Moreover, their activities transcend multiple blockchains. At the INTERPOL New Technologies Forum in October 2023, Merkle Science presented findings that TRON has accounted for approximately 90% of funds associated with terrorist financing since 2021. The pattern of use, in conjunction with the extent to which these are available on the dark web and the importance of cryptocurrency as an enabler for cybercrime, suggests it is highly likely these services are being used. This presents significant opportunities for investigations, considering the increasing effectiveness of blockchain and cryptocurrency analytical tools.

Cybercrime-as-a-Service

The Cybercrime-as-a-Service model is both complex and extensive, covering a wide range of services. While the research confirms threat actors with motivations other than financial considerations do interact with these services, the extent of this interaction is again hindered by the data access and attribution challenges. Nonetheless, based on the research conducted, certain specific services stand out, and are described in the subsections that follow.

1.   DDoS-as-a-Service

There is a well-documented use of DDoS services to disrupt entities that diverge from shared political, religious, or general views. The DDoS-as-a-Service model has been a key enabler in this regard, and it is certainly the standout example of cybercrime-as-a-service in the context of non-financially motivated threat actors.

---

105   https://www.elliptic.co/resources/terrorist-financing-and-cryptoassets-in-2023

Despite law enforcement interventions such as "Operation Poweroff,"[106] the number of available services continues to grow. Notably, threat actors are not only users but also developers. This dates to 2015, when LizardSquad, which claimed to support Da'esh, created their own DDoS stressor tool.[107] This has persisted as a trend, with threat actors increasingly developing and sharing such tools within their communities. Dissemination often occurs through public Telegram channels, where developers actively promote their creations and encourage additional attacks by followers and volunteers.[108] Futhermore, the commodification is further promoted by groups that may not be the original developers but leverage existing tools to offer DDoS services. Such tools advocated for by noteworthy threat actors include Skynet DDoS tool, Kryptos, and Ddosia.[109]

2.   Stolen Data-as-a-Service

Many threat actors seek, in the pursuit of their goals, to generate fear by showcasing the vulnerability of infrastructure and stealing data. Those involved appear to possess skills in network intrusion, yet there is insufficient information to confirm the extent to which they may utilize Access-as-a-Service to enable their activities.

Stolen data is of course a beneficial by-product of a cyber-attack that can be sold. In addition to the previously mentioned Ferizi example, another example of a threat actor exploiting such data is "Bjorka,'" who targeted ministries in a Southeast Asian country, hacking their systems for sensitive data and selling it on specialized dark web cybercrime forums.[110] Such stolen data is often offered on independent dark web domains, cybercrime forums, or published on encrypted communication platforms, typically Telegram. While the preceding examples show the onward sale of stolen data, there are also instances where threat actors with non-financial motivations make it available at no cost. Ultimately, the goal is to further facilitate disruption and raise awareness of the cause.[111]

3.   Ransomware-as-a-Service

While limited evidence links non-financially motivated threat actors' activity to RaaS, it warrants attention as a growing and high-impact threat. Although the primary motivation behind ransomware has been financial, some indications suggest that threat actors with non-financial motivations are also entering this space. In 2020, the G7 explicitly mentioned this in the context of terrorist financing, highlighting the risk that ransomware proceeds could be used to finance terrorism once they have been converted from a victim account into anonymously

---

106   https://www.europol.europa.eu/media-press/newsroom/news/global-crackdown-against-ddos-services-shuts-down-most-popular-platforms

107   https://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/

108   https://flare.io/wp-content/uploads/The-Typology-of-Illicit-Telegram-Channels.pdf

109   https://www.slcyber.io/attack-for-hire-services-the-evolution-of-ddos/
https://socradar.io/dark-web-profile-noname05716/

110   https://thediplomat.com/2022/09/bjorka-the-online-hacker-trying-to-take-down-the-indonesian-government/

111   https://www.usip.org/sites/default/files/sr119.pdf

held funds and transferred into an unidentified cryptocurrency wallet.[112] Furthermore, terrorists may seek inspiration from criminal activities in this area. For example, the hacker group GhostSec, known for its self-declared vigilante activities, has introduced a new RaaS model called GhostLocker.[113] This service is offered on the dark web at a price of USD 999 for access to 15 slots during its beta phase, or instances of the ransomware that a buyer can acquire for their use, with a post-beta price set at USD 4,999. Other groups have expressed their intention to utilize this service.

The scarcity of examples of non-financially motivated RaaS might be linked to the increased complexity of ransomware compared to less sophisticated cyber-attack types like DDoS. However, the risks heighten as more cyber-skilled actors converge around shared belief systems for opportunistic reasons. The potential threat posed by the use of RaaS by threat actors for reasons other than financial is significant, given the overall rise to prominence of ransomware in general and its demonstrated impact since this attack type first emerged. This is particularly true when it comes to critical infrastructure, where even a single instance of RaaS deployed by threat actors could cause significant damage.

4.   Threat-as-a-Service

Threat-as-a-Service (TaaS) is a model that involves the provision of multiple cybercrime-as-a-service products and services on one platform or as a package, thus facilitating convenient access to wholesale cyber capabilities. It was first unveiled as the next generation of services under development on a cybercriminal group's Telegram channel and entailed an offering of a comprehensive solution, including Stealer, Ransomware, Pen-Test Tools, and DDoS capabilities – all in one place.[114] Despite being relatively new and having limited evidence, this is noteworthy as a potential threat, particularly in cases where threat actors previously focused on DDoS can now access elements such as ransomware.[115]

---

112   https://home.treasury.gov/system/files/136/G7-Ransomware-Annex-10132020_Final.pdf

113   https://socradar.io/ghostlocker-a-new-generation-of-ransomware-as-a-service-raas/

114   https://socradar.io/mother-of-the-threats-threat-as-a-service/#:~:text=Anonymous%20Russia's%20botnet%20service%20Tesla,and%20Tesla%20Bot's%20DDoS%20features.

115   https://socradar.io/mother-of-the-threats-threat-as-a-service/

Pulling the Threads Together

This study set out to address the knowledge gap in terms of terrorism and violent extremism in the cybercrime underground by shedding light, in particular, on the activities in the dark web and the development of cybercrime-as-a-service, which has become prevalent in the dark web ecosystem. In attempting to do so, the research has highlighted the fundamental challenge of attribution faced by law enforcement agencies in carrying out dark web investigations in the context of counter-terrorism. The inability to exhaustively and definitively scope the type and actual extent of the linkages with the dark web marketplaces and cybercrime-as-a-service does not imply that such connections do not exist. In fact, the evidence presented in this report, even if limited, suggests otherwise. There is evidence that threat actors with motivations other than financial are engaged in the dark web and with cybercriminal elements in the context of cybercrime-as-a-service. They themselves are sometimes providers of the services, and considering terrorist groups have established cyber strategies, it can, be reasonably assumed that these groups are likely engaged on the dark web and the broader cybercrime underground, and that cybercrime-as-a-service is or could become a key enabler of cyber-attacks by terrorists through the sale of the required services and products, and even 'all-inclusive' packages. This challenges the established belief that the threat of more advanced cyber-enabled terrorist attacks is low simply because these groups and individuals have themselves limited cyber-attack capabilities.

Examining non-financially motivated threat actors – as distinct from those primarily motivated by profit – has also shed light on the risk of convergence that fuels the threat of terrorism and violent extremism related cyber-attacks. Such convergence, from strictly opportunistic to potentially facilitated by ideological affinities, highlights the interconnected nature of modern threats and represents a significant challenge for counter-terrorism. It is, therefore, crucial to further explore the interplay between financially motivated cybercriminals and threat actors with motivations other than financial – recognizing at the same time that neither group is exclusively homogeneous and that some actors may not fall squarely in either category.

The well-established attribution challenge is also further compounded when considering the possible overlapping and dynamic nature of financially motivated cybercriminals and otherwise motivated threat actors using the dark web and the broader cybercrime underground. Cyberattacks might be labelled as financially motivated, whereas there could have been other, non-financial, motivations behind the choice of the target hidden within the criminal underground. These individuals and their motivations are often indistinguishable when operating either as individuals or groups and can change over time and depending on specific situations. The collaborative nature of some groups or collectives adds further complexity, both in terms of the scale of the threat and attribution, as anyone with the relevant cyber-skills can collaborate to enable a cause. Therefore, the threat essentially encompasses anyone with cyber-skills capable of redirecting their expertise to attacks when suitable and leveraging the extensive resources within the dark web, the broader cybercrime underground, and the cybercrime-as-a-service model.

Recommendations

Having explored the dark web, the broader cybercrime underground, and the potential role of cybercrime-as-a-service from the perspective of threat actors motivated by considerations other than financial, the overarching takeaway should be the need for a strategic approach to the threat, ensuring security and law enforcement agencies, and specifically those mandated with countering terrorism and violent extremism, are best positioned to prevent and investigate such activities. Beyond this, several specific recommendations have been identified and are described in the following subsections.

Complementing, and indeed, allowing for the adoption of a strategic approach to the threat is the need for appropriate legal mandates for law enforcement and counter-terrorism agencies to conduct investigations, which in many ways underpins each of the specific recommendations presented below. In conjunction with the need for legal mandates and recognizing the reality that most investigations will entail the collection and processing of personal information, and consequently may interfere with a range of human rights, it is important to also highlight the critical importance of ensuring that relevant measures taken are human rights-compliant, including through the establishment and implementation of robust human rights safeguards.

1.   Understanding the Threat

The central recommendation in addressing the challenges associated with the evolving cyber threat landscape is to enhance cyber situational awareness. This stems from the recognition of a prevailing lack of understanding regarding emerging threats and attribution. Foremost, to achieve this, it is crucial to acknowledge that Tor is just one tool in the cybercrime toolkit, and there is a need for a more comprehensive approach to data collection and analysis across the wider criminal underground.

To effectively delve into the intricacies of the cybercrime underground, there is also a need to collect and analyze larger datasets to enable more proactive approaches and the discovery of emerging threats. During the research, several advanced data-gathering tools were encountered. It was evident that many of them are experimenting with further enhancements to encompass both the wider criminal underground and more proactive discovery. The use of AI is also being explored. For example, DarkBert, an initiative supported by INTERPOL, is a specialized AI model adapted to process and interpret text from the dark web, focusing on understanding the unique language and slang. While these developments hold promise for bolstering AI capabilities and, in turn, improving the understanding of the threat, additional efforts are required to refine and optimize these tools for more effective use in combating cyber threats and to ensure that these tools do not lead to unlawful infringements of human rights.

This expanded scope requires going beyond readily accessible information and venturing into more restricted areas. In addressing this limitation, it is imperative to recognize the significance of human intelligence in understanding and infiltrating the more restricted areas of the cybercrime underground. While some commercial entities provide investigation intelli-

gence, the capabilities for this are highly specialized and come at a considerable cost, often surpassing the budgets of many organisations. Government agencies with a prescribed law enforcement or investigative mandate can also conduct such activities, but they, too, face resource and legal constraints.

To overcome challenges for understanding the full scope of the threat, it is recommended to further explore avenues for improving the data collection and analysis limitations and developing relevant approaches that are consistent with international human rights norms and standards. This can include the establishment of working groups and facilitation of coordination among private sector and civil society organizations working on the dark web and encrypted channels of data collection and analysis, in order to foster collaboration with the public sector. This would seek to bridge knowledge gaps, promote information-sharing and proactive identification of emerging threats. By creating a more cohesive and coordinated approach, stakeholders from both sectors can collectively enhance their ability to navigate and respond effectively to the dynamic landscape of cyber threats.

2.   Cybercrime Investigation Capabilities

Training

In the contemporary landscape of technology-driven operations, it is imperative that all relevant teams within law enforcement and counter-terrorism agencies possess a foundational understanding of cybersecurity and open-source investigations. Basic training is not just advisable but essential to empower personnel with the knowledge and skills required to navigate the evolving challenges posed by cyber threats. This training should encompass key areas such as cybercrime, entry-level data science, digital forensics, dark web, and cryptocurrency investigations to equip individuals with a well-rounded comprehension of the cyber landscape, as well as considerations of the human rights dimensions to support law enforcement and counter-terrorism officials to act in compliance with relevant international human rights norms and standards.

A fundamental grasp of cyber threats enables law enforcement and counter-terrorism personnel to recognize and respond effectively to potential risks, creating a more robust front line of defence against malicious activities. This level of understanding is crucial across all law enforcement agencies. For example, a non-cyber specialized search officer should be able to recognize and comprehend the significance of a seed phrase[116] in securing cryptocurrency wallets. Such awareness not only enhances their knowledge of the threats and their ability to carry out their duties effectively but also contributes to an organisational culture that prioritizes cybersecurity.

While not every team member needs to become an expert in advanced areas like data science, cryptocurrency tracing, or digital forensics, a foundational knowledge base is indispensable. This ensures that employees across various departments can communicate effectively and collaborate seamlessly in addressing cybersecurity concerns. In this context, a case officer, for instance, should possess enough knowledge to engage with and extract meaningful insights from digital forensics officers efficiently.

Furthermore, law enforcement and counter-terrorism agencies should invest in advanced training for specialists dedicated to roles directly involved in cybersecurity, such as data scientists, blockchain analysts, open-source investigations, and forensic experts. This advanced training ensures that these specialists stay at the forefront of emerging threats and technologies, maintaining a high level of expertise where it is most needed.

In light of the increasing complexity of modern crime and security challenges, the need for comprehensive frameworks to guide law enforcement capabilities is paramount. Recently, UNOCT's joint initiative with INTERPOL, CT TECH, released a report detailing a robust framework for assessing and enhancing law enforcement capabilities. This report outlines a systematic approach for Member States to evaluate their existing capacities, identify gaps, and implement strategies for improvement in their use of new technologies. This report should be read in conjunction with CT TECH report focused on adopting a human rights-based approach to countering the use of new technologies for terrorist purposes. By leveraging the insights and methodologies provided in these reports, Member States can effectively bolster their law enforcement capabilities to better tackle evolving threats and ensure the safety and security of their citizens.

Tools, Tactics and Techniques

Addressing the threat of cyber-attacks requires not only knowledge, but also well-equipped teams with access to a comprehensive array of tools, tactics, and techniques. This arsenal encompasses not only open-source information collection and data analysis tools, but also extends to digital forensics and cryptocurrency tracing tools. Digital forensic tools can play a pivotal role in the aftermath of cyber incidents, aiding in the extraction and analysis of data which can improve the understanding of the modus operandi - information that is crucial

---

116   A series of random words generated by a cryptocurrency wallet that secures access to the funds in that wallet. These words can be written on paper, stored in a file on a device, or even imprinted into metal to protect from fire damage. Seed phrases are often 12, 24, or 25 words and are required to access, recover or seize cryptocurrency wallets.

in devising effective countermeasures and providing the means to attribute cyber-attacks. Cryptocurrency tracing, on the other hand, allows for tracking the flow of funds, identifying clusters of addresses associated with illicit activities, and uncovering patterns indicative of money laundering, thereby shedding light on cyber-attacks and links to the dark web and cybercrime-as-a-service. Despite hurdles posed by privacy-centric cryptocurrencies and obfuscation techniques, cryptocurrency tracing remains pivotal in combating the threats, necessitating strategic investment by counter-terrorism agencies. However, it should be noted that the level of effectiveness of cryptocurrency tracing depends on the quality of entity enrichment – a process that involves adding identifiable labels to wallets and addresses. This further emphasizes the need for enhanced data science capabilities and cross-sector information-sharing.

3.   Promoting Shared Operational Expertise

Effectively addressing technical threats requires a multifaceted approach, and a comprehensive defence against these threats demands a combination of cybersecurity expertise, cybercrime and counter-terrorism proficiency, and technical acumen. Often, these distinct skills do not converge in a single person, necessitating collaboration across specialized roles, as capacity-building alone may be insufficient to meet the nuanced needs of threat mitigation.

Therefore, it is recommended to establish frameworks that foster closer cooperation and shared expertise between counter-terrorism units, cybercrime investigators, and technical specialists. A harmonized approach to technical threat mitigation involves recognizing the distinct expertise required and fostering collaboration between counter-terrorism, cybercrime, and technical capabilities. Establishing frameworks for cross-disciplinary cooperation and optimising the deployment of technical expertise contribute to a more efficient and resilient defence against the multifaceted challenges posed by evolving technical threats.

Such a collaborative approach will help to ensure a holistic understanding of the threats, facilitating a more comprehensive and coordinated response. By breaking down silos and promoting cross-disciplinary collaboration, organisations can enhance their ability to detect, prevent, and respond to technical threats effectively.

The importance of technical expertise cannot be overstated, which in itself is cross-disciplinary. Digital forensic experts, data scientists, and crypto-tracers bring unique skill sets that, when combined, create a formidable defence against today's digital threat landscape. Managing technical expertise effectively involves deploying these resources in a strategic and coordinated manner to ensure a more cost-effective means of maintaining and servicing the evolving security needs, and, indeed, guaranteeing that related skills are continuously updated and adapted to keep pace with evolving technical developments and methodologies.

4.   Facilitating Joint Activities

Information-sharing is not always optimal between government entities and private industry, yet international cooperation and public-private sector partnerships stand out as pivotal elements in addressing the multifaceted challenges posed by cyber threats – as specifically called for in the United Nations Global Counter-Terrorism Strategy. To address these challenges, various strategies have been employed, such as strategic workshops, platforms for information sharing, public-private sector collaboration initiatives, and operational surge activities. Each of these approaches plays a unique role in enhancing understanding, prioritisation, and mitigation of cyber threats:

- Strategic workshops provide forums for stakeholders from different nations and sectors to come together, share insights, and collaboratively develop strategies to address emerging cyber threats. These workshops foster a deeper understanding of the evolving threat landscape and facilitate the exchange of good practices and expertise.

- Platforms for information-sharing serve as crucial mechanisms for disseminating timely and relevant information about threats. Promoting open communication and sharing insights, can bolster defences against cyber threats globally.

- Public-private sector collaboration initiatives further strengthen these efforts by bringing together governmental agencies and private entities, leveraging the strengths of both sectors to enhance cybersecurity measures. In line with the imperative for international cooperation and public-private partnerships in addressing cyber threats, the

Guide for Establishing Law Enforcement Cooperation with Technology Companies in Counter-Terrorism, developed under UNOCT's joint initiative with INTERPOL, CT TECH, serves as a valuable resource. The guide emphasizes the importance of optimizing information sharing between government entities and private industry, based on various models of collaboration, while recognizing it as a fundamental component in addressing the multifaceted challenges posed by cyber threats. Drawing from various strategies employed to enhance collaboration and response, the guide provides actionable insights for fostering effective partnerships.[117]

1. INFORMATION SHARING

Set up to exchange threat information in real time, in a secure, confidential and dynamic environment, and increasing situational awareness and key trends

2. CAPABILITY AUGMENTATION

Outsource key capabilities and services to private technology companies which are needed by law enforcement

3. BUSINESS ALLIANCE/COUNCIL

Broad collaboration model between law enforcement and private technology companies or industry to enhance general awareness, prioritize mutual areas of interest, and to collaborate in countering terrorist use of new technologies

4. ACTIVE INVESTIGATION

Cooperation model between law enforcement and technology companies to support active investigations in the disruption and prosecution of terrorist

TABLE 4. Models of Cooperation	
Information Sharing	Facilitate bi-lateral information sharing to include exchanging relevant threat information, understanding terrorist trends and tactics in using technology for malicious activities, alerting and taking action on suspicious or illegal behaviour. Additionally, it is important to prioritize identifying threats related to terrorist abuse of Information and Communication Technology (ICT) company services, platforms, or products. By prioritizing these aspects, the cooperation can effectively address the challenges posed by terrorist activities.
Capability Augmentation	Commercial companies provide intelligence-gathering services to the intelligence community for a fee, investing resources and technology in various fields such as the darknet or cryptocurrency. Collaborating with such companies could be beneficial for both parties, as many have developed capabilities that law enforcement agencies (LEAs) can use to combat terrorism more effectively.
Business Alliance / Council	Establishing a business alliance aims to enhance the capabilities of fighting terrorism by sharing technologies and techniques, and gaining knowledge about potential threats. This collaboration can assist LEAs in better preparation for upcoming threats and provide insights into future developments to mitigate terror risks. The primary objectives of this council are to explore potential risks and opportunities that future technologies may unfold.
Active Investigations	The main goal of cooperation between LEAs and ICT companies is to collect data related to terrorist investigations and prevent terror groups from abusing their services. This cooperation is crucial for enhancing public safety through prevention and prosecution.

Table 1: Establishing Law Enforcement Capabilities with Technology Companies in Countering Terrorism – CT TECH Initiative

---

117   https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_establishing_law_enforcement_web.pdf

- Operational surge activities, particularly those focused on the cybercrime underground, are exemplified by initiatives such as the European Union Agency for Law Enforcement Cooperation (Europol)'s Joint Referral Action Days Operations, including the one conducted in collaboration with Telegram in 2019.[118] These initiatives entail concentrated efforts, including multiple agencies, to identify and disrupt illegal activities conducted on the criminal underground. These initiatives, when executed jointly by law enforcement agencies and the private sector, prove to be effective in combating cybercriminal networks.

Such types of operational surge activities, especially those involving the cybercrime underground, should be advocated for and promoted. Proactive coordination with relevant agencies, utilizing the support from multilateral platforms like INTERPOL and Europol, is essential to ensure a cohesive and synchronized approach to tackling global cyber threats. By facilitating collaboration between law enforcement and private entities, law enforcement agencies can pool resources, share intelligence, and collectively enhance their capabilities to combat cyber threats on a global scale. Emphasising meaningful and human rights-compliant international cooperation and public-private partnerships is key to building a resilient and collaborative front against the constantly evolving landscape of cyber threats.

5.   Respecting and Protecting Human Rights

Under international law, States have an obligation to take appropriate measures to protect persons within their jurisdiction against reasonably foreseeable security threats posed by third parties, including terrorist actors, while ensuring that measures taken for that purpose respect and protect human rights. Efforts undertaken by law enforcement and counter-terrorism agencies to gather intelligence, collect, store, use and share data, monitor and investigate the use of the dark web by terrorists and violent extremists may encroach on a number of rights, including, for instance, the right to privacy, data protection, or the right to freedom of expression. In the absence of universally agreed definitions of terrorism and violent extremism, vague and overly broad definitions at the domestic level may be abused by States to target activities of civil society actors, human rights defenders, journalists, and political opponents who are resorting to the dark web for security, anonymity, and confidentiality purposes.

It is therefore crucial that legislative frameworks governing measures to counter the convergence of terrorism, violent extremism and cyber-criminality on the dark web are precise, clear, accessible, foreseeable, and contain adequate safeguards against abuse. Any interference with human rights must be provided by law, necessary to protect a legitimate aim, proportionate and must respect the prohibition against discrimination. Independent, effective, adequately resourced and impartial oversight mechanisms should be established to ensure transparency and accountability for States' practices aimed at countering the use of the dark web for terrorist purposes. States and private sector businesses have human rights obligations and responsibilities, respectively, that apply to the context of countering terrorism and

---

118   https://www.europol.europa.eu/media-press/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online

violent extremism both offline and on the dark web.

Annex

The following outlines privacy-focused software. The examples provided are legitimate services at the time of writing and included exclusively for explanatory purposes. They do not hold any particular significance in terms of illicit activity.

Category of Privacy-Focused Software	Examples (in alphabetical order)
Virtual Private Networks (VPNs)	CyberGhost, ExpressVPN, IVPN, Mullvad, NordVPN, ProtonVPN, Surfshark, VyprVPN, etc. Features: no logs policy, location jurisdiction, independent auditing
Privacy-orientated browsers	Brave, DuckDuckGo, Iridium, Waterfox etc. Features: protection against tracking, fingerprinting, and other privacy-invasive practices common on the Internet
Operating systems that prioritize anonymity	Graphene (for Android), Parrot Security, Tails, Qubes (based on Whonix), Whonix Features: default routing of Internet via Tor encryption, enhancement with privacy tools, compartmentalization
Encrypted communication platforms	Sometimes known as "messaging apps" such as Discord, Dust, Signal, Telegram, Threema, Viber, WhatsApp, Wire, Wickr, and self-hosted communication platforms like Mattermost, Rocket Chat, Zullip etc. Key features: encryption of the communications traffic

Category of Privacy-Focused Software	Examples (in Alphabetical Order)
Private email services	HushMail, Mailfence, MsgSafe, Posteo, ProtonMail, Runbox, Tutanota Features: encryption including zero access for providers, location jurisdiction, no logs policy, payment anonymity
Secure file storage solutions	Popular cloud storage: AWS, Box, Drive, Dropbox, Google OneDrive, iDrive, NextCloud, Proton Drive, SmartVault, Peer-to-peer (P2P) solutions like BitTorrent, DC++, FilePizza, InterPlanetary File System (IPFS), uTorrent, Vuze Anonymous file sharing: Jirafeau, LocalSend, Mega, OnionShare, Swiss Tresorit, Syncthing, Send, Transfer, Wetransfer
Decentralized networks	Various types such as ones that focus on social networks: Bluesky, Lens Protocol, Odysee, PixelFed General web-like networks: Freenet, Invisible Internet Project (I2P), Zeronet Cryptocurrency: Bitcoin, Ethereum, Monero