LmunA 2024

Research report

Forum: GA1

Issue: Addressing the growing cybersecurity threats faced by journalists

Student Officer: Cecilia Passa

Position: Deputy Head

LMUNA
Lorentz Lyceum
Model United Nations
Arnhem

Introduction

LmunA 2024

Currently, the digital security of publishers, journalists and their sources are under threat in many parts of the world due to cybersecurity threats[1]. Consequently, cybercrime has become a growing concern among policymakers in many parts of the world. More specifically, as of 2021, the UN Conference on Trade and Development found that 80% of countries had enacted cybercrime legislation. Academic and public attention to cybercrime, ransomware, and spyware have also grown, both in the wake of prominent attacks and amid growing concerns about the adoption of generative AI technologies in cyberattacks.

Nevertheless, widespread uptake of digital security tools has been limited due to a lack of resources, funding and technological infrastructure as well as how difficult it can be to navigate complex, less user-friendly technologies. Even in highly digital environments, those with less developed infrastructures may have insufficient capacity to protect against cyber threats. Even so, the ability to mitigate digital security risks differs across countries and newsrooms[2].

With specific regards to cybersecurity threats faced by journalists, cyber-attacks on media entities, even those that have a relatively minor impact or are unsuccessful, are highly visible to the public compared to other sectors. Media platforms are the prime target for hacktivists who wish to push out messages to the wider public. Following the Russian invasion of Ukraine in February, for instance, pro-Ukrainian groups took over Russian TV channels to broadcast messages opposing the Kremlin's actions. "News outlets are frequently targeted by politically motivated actors who aim to disrupt or compromise the content and its distribution," commented Dan Vasile, VP of strategic development at BlueVoyant[3].

The nature of journalism as an incredibly public-facing and accessible occupation gives rise to specific risks for those in the industry. Digital security threats include online harassment and abuse, and doxing campaigns against journalists which makes journalists and their contact information easy to access online. Therefore, this greatly threatens the freedom of the press, and as Albert Camus reported: "A free press can, of course, be good or bad, but, most certainly

---

[1] "Journalists & Online Abuse." Center for News, Technology & Innovation, 22 July 2024, www.innovating.news/article/journalists-online-abuse/.

[2] "Journalists & Cyber Threats." Center for News, Technology & Innovation, www.innovating.news/article/journalists-cyber-threats/.

[3] Coker, James. "Cyber-Attacks in the Media Industry Making Headlines." Infosecurity Magazine, 13 Mar. 2023, www.infosecurity-magazine.com/news-features/cyber-attacks-media-industry/.

without freedom, the press will never be anything but bad.[4]" One thing is clear: cybersecurity threats faced by journalists need to be minimised and eradicated immediately through a cooperation of all relevant stakeholders.

Definitions of key terms

Cybercrime

"There is no single, internationally accepted definition of cybercrime or cyberattacks. The definition may include crimes dependent on the use of technology, crimes facilitated by the use of technology or both. Limitations to this definition may be set based on the seriousness of the crime or the type of case (e.g., criminal, civil, administrative or all of the above).[5]"

Cybersecurity threat

"Cybersecurity threats are acts performed by individuals with harmful intent, whose goal is to steal data, cause damage to or disrupt computing systems. Cyber threats can originate from a variety of sources, from hostile nation states and terrorist groups to individual hackers, to trusted individuals like employees or contractors, who abuse their privileges to perform malicious acts.[6]"

Cyberattack

"An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.[7]"

Software

"Software is a set of instructions, data or programs used to operate computers and execute specific tasks.[8]"

Spoofing

---

[4] "The Deluge of Digital Attacks against Journalists." The Cloudflare Blog, 3 May 2022, www.blog.cloudflare.com/the-deluge-of-digital-attacks-against-journalists.

[5] "Journalists & Cyber Threats." Center for News, Technology & Innovation, www.innovating.news/article/journalists-cyber-threats/.

[6] Imperva. "Cyber Security Threats | Types & Sources | Imperva." Imperva, 2022, www.imperva.com/learn/application-security/cyber-security-threats/.

[7] Editor, CSRC Content. "Cyber Attack - Glossary | CSRC." Csrc.nist.gov, www.csrc.nist.gov/glossary/term/cyber_attack#:~:text=An%20attempt%20to%20gain%20unauthorized.

[8] Rosencrance, Linda. "What Is Software? Definition, Types and Examples." SearchAppArchitecture, Mar. 2021, www.techtarget.com/searchapparchitecture/definition/software#:~:text=Software%20is%20a%20set%20of.

"Spoofing is a type of cybercriminal activity where someone or something forges the sender's information and pretends to be a legitimate source, business, colleague, or other trusted contact for the purpose of gaining access to personal information, acquiring money, spreading malware, or stealing data.[9]"

General overview

The issue

The physical and digital security of journalists and their sources are under threat in many parts of the world. Digital security and cybersecurity threats have become more important than ever for the global news media as journalists and publishers are becoming high-profile targets for malware, spyware and digital surveillance, compromising their and their sources' personal information and safety. One prominent example of a high-profile smartphone-related threat is that of the NSO Group's Pegasus spyware. Clients of the Israeli technology firm, including various national government officials, reportedly identified many journalists as surveillance targets, in countries including Canada and Mexico[10]. More broadly, digital security and cybersecurity have gained the attention of policymakers globally, with 156 countries having enacted cybercrime legislation as of 2021[11].

Sources of Cybersecurity Threats

The sources of cybersecurity threats are multiple and diverse, ranging from terrorist organizations to malicious insiders. For example, hostile countries can launch cyber-attacks against local companies and institutions, aiming to interfere with communications, cause disorder, and inflict damage. Equally, terrorists conduct cyber-attacks aimed at destroying or abusing critical infrastructure, threatening national security, disrupting economies, and causing bodily harm to citizens. Criminal groups often break into computing systems for economic benefit through phishing, spam, spyware and malware for extortion, theft of private information, and online scams. Furthermore, individual hackers target organizations using a variety of attack techniques. They are usually motivated by personal gain, revenge, financial gain, or political activity. Hackers often develop new threats, to advance their criminal ability and improve their personal standing in the hacker community. Finally, malicious insiders, or employees who have

---

[9] "What Is Spoofing?" Cisco, www.cisco.com/c/en/us/products/security/email-security/what-is-spoofing.html#:~:text=Spoofing%20is%20a%20type%20of.

[10] Shere, Anjuli, et al. "How the Internet of Things Poses a Threat to Journalists." The Journalist's Resource, 1 Nov. 2021, www.journalistsresource.org/home/how-the-internet-of-things-poses-a-threat-to-journalists/.

[11] "Journalists & Cyber Threats." Center for News, Technology & Innovation, www.innovating.news/article/journalists-cyber-threats/.

legitimate access to company assets, can abuse their privileges to steal information or damage computing systems for economic or personal gain. Insiders may be employees, contractors, suppliers, or partners of the target organization. They can also be outsiders who have compromised a privileged account and are impersonating its owner[12].

The method of cybersecurity threats:

Cybersecurity threats are carried out with a variety of methods, each one of which is meticulously used depending on the situation[13].

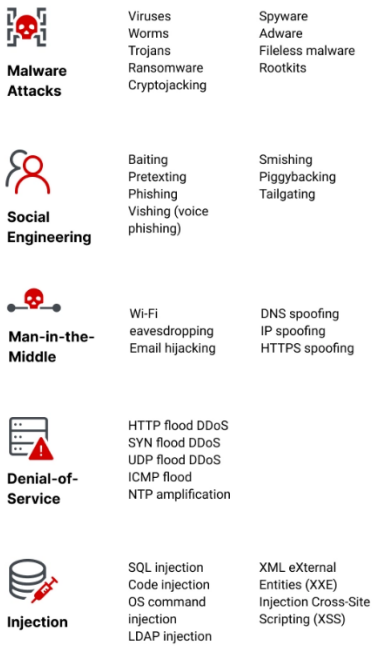

Figure 1: All the methods that cybersecurity attacks are carried out by[14]

Malware

Malware, or "malicious software," refers to viruses, worms, or Trojan horses that can be put into a system through an untrusted website link, unsolicited software download, or via an email. It is installed on the target system, after which it collects private information, modifies and blocks access to network entities, and can erase information and even shut down the computer. It is

---

[12] Imperva. “Cyber Security Threats | Types & Sources | Imperva.” Imperva, 2022, www.imperva.com/learn/application-security/cyber-security-threats/.

[13] “Journalists & Cyber Threats.” Center for News, Technology & Innovation, www.innovating.news/article/journalists-cyber-threats/.

[14] Imperva. “Cyber Security Threats | Types & Sources | Imperva.” Imperva, 2022, www.imperva.com/learn/application-security/cyber-security-threats/.

possible to further sub-categorize malware assaults into smaller classes, such as worms or viruses.

- Worms are pieces of malware that exploit holes in software to gain entry to an operating system and commandeer it.
- Trojan horses are programs or code with malicious intent, which are hidden in other seemingly benign programs and come mostly as attachments to emails, games, and applications. The user, unknowingly, downloads the trojan and authorizes the latter to hijack the former's device.
- Ransomware entails using encryption to intentionally deny a user or organization access to their own systems or data. The attacker would usually demand a decryption key in return for the payment of a ransom but does not guarantee that the systems would be functional again or that all data would be restored upon payment.
- In the cryptojacking case, a bad actor executes software on the target machine and uses it to mine cryptocurrency on behalf of the target without their knowledge. Also, cryptojacking kits cause the affected systems to be slow; they are to partly blame for system stability.
- Spyware is essentially how a threat actor gains access to sensitive information of an unknowing user—some of this information might be passwords, while some of it might be payment details. Spyware could be on mobile, or desktop-app based or even on desktop browsers.
- Adware allows advertisers to provide the user, by following the user's activity in a bid to determine patterns and interests, with targeted advertisements. The use of adware, unsanctioned by the users may compromise their privacy.
- When the operating system has no installed software, it is known as fileless malware. Malicious functions are enabled through editing native files, such as PowerShell and WMI. Antivirus programs are unable to detect this type of assault since the infected files are accepted as authentic.

Social Engineering Attacks

Social engineering is the art of convincing people to allow viruses entry points into their device. Since the attacker is spoofed to be someone reputable, the victim is unaware, downloading malware into his/her device or sensitive information.

- The attack—named "baiting"—is when a user is lured into doing something that will eventually put themselves in the attacker's trap under the promise of some goodie, perhaps a gift card. The victim gives out sensitive information to the attacker.
- Pretexting is a means through which an attacker enforces the victim to give out information based on false pretences. Normally, it involves acting like an authoritative individual, such as a police officer, whose position will compel the victim to act in obedience.
- Phishing consists of an attacker sending emails to many users, masquerading as a source that is trustworthy; the emails can also be more specifically targeted. For instance, "whaling" targets persons of high value, such as CEOs, but "spear phishing" targets the email to a specific user. Vishing, also known as voice phishing, is where the target is called by the imposter in an attempt to get them to grant access to their system or to reveal private information. Anyone can fall victim to vishing, but generally, it targets older people. Smishing is where the attacker sends text messages to trick the victim.
- When an individual "piggybacks" on the credentials of an authorized user, the authorized user offers the individual physical access.

Supply Chain Attacks

The attacks on supply chains are a new threat targeting vendors and software developers. Its objective is to spread malware through source code, build processes, or update methods of software applications to infect the legitimate apps. Attacks accomplish this by exploiting vulnerabilities in server architecture, coding practices, and insecure network protocols to infiltrate build and update processes, change source code, and obscure the delivery of malicious content. Supply chain attacks are quite dangerous because the corrupted applications are signed and validated by reliable providers. In a software supply chain attack, the software vendor is unaware that its updates or applications contain malware.

Man-in-the-Middle Attack

A Man-in-the-Middle attack is an attack wherein the attacker intercepts the communication between the two endpoints: for example, a user and an application. In doing so, he can impersonate each entity of the conversation to each other, listen to it, and capture vital information.

- Wi-Fi eavesdropping: An attacker may create a Wi-Fi connection, which would be accessed by people and who would naturally assume it as the network of some trusted entity, like a company. All activities of the connected users are then trackable, and

sensitive information, such as payment card numbers or login credentials, can be intercepted with the fake Wi-Fi.

- Email hijacking involves spoofing the e-mail address of some real organization, such as a bank, and sending it to consumers in a bid to fool them into giving out private information or sending the attacker money. The user thinks he is complying with the bank's instructions but actually is following those of the attacker.
- In domain name server spoofing, a user is directed to a malignant website that impersonates the legal website. In such scenarios, the hacker either takes the credential of the user or reroutes the traffic away from the trustworthy website.
- IP spoofing is a technique in which the hacker identifies himself as a website and further misleads the user into believing that he is dealing with the website.
- HTTPS is generally considered the more secure version of HTTP, but can also be used to trick the browser into thinking that a malicious website is safe in HTTPS spoofing. The attacker uses “HTTPS” in the URL to conceal the malicious nature of the website.

Denial-of-Service Attack

A Denial-of-Service attack disrupts the normal operation of the victim system by flooding it with too much traffic. A DDoS attack is simply an attack that utilizes multiple ordinal devices.

- An HTTP flood denial-of-service attack is simply a phase of HTTP requests against a web server or any application layer 7 resource. There is no bandwidth required, and neither are corrupt packets involved in the attack, the main tactic of which would be to enforce the target system to use all resources it can handle for every request.
- A Transmission Control Protocol connection sequence sends a SYN request to which the host has to respond by sending a SYN-ACK acknowledging the request, and the requester replies with an ACK. This creates a SYN flood DDoS. Attackers can leverage this sequence by sending SYN requests and remaining deaf to the host's responding SYN-ACKs, paralyzing server resources.
- A flood of UDP DDoS is a type of attack whereby there is a huge transmission of UDP packets to random ports on a remote computer. This technique eats up host resources and forces the host to search for applications on the affected ports and respond with "Destination Unreachable" packets.
- Where the destination is overwhelmed or overrun with an abundance of ICMP Echo Request packets, the situation is called an ICMP flood. This slows down the system

where the servers can't keep up with the requests that are being sent even though they may try to respond to every request with an ICMP Echo Reply packet.

- When Network Time Protocol (NTP) servers are publicly available and an attacker can use this to transmit massive amounts of UDP traffic to a targeted server, it is known as NTP amplification. The query-to-response ratio of 1:20 to 1:200, which enables an attacker to take advantage of open NTP servers to launch high-volume, high-bandwidth DDoS attacks, makes this attack an amplification.

Injection Attacks

Injection attacks exploit a variety of vulnerabilities to directly insert malicious input into the code of a web application. Successful attacks may expose sensitive information, execute a DoS attack or compromise the entire system.

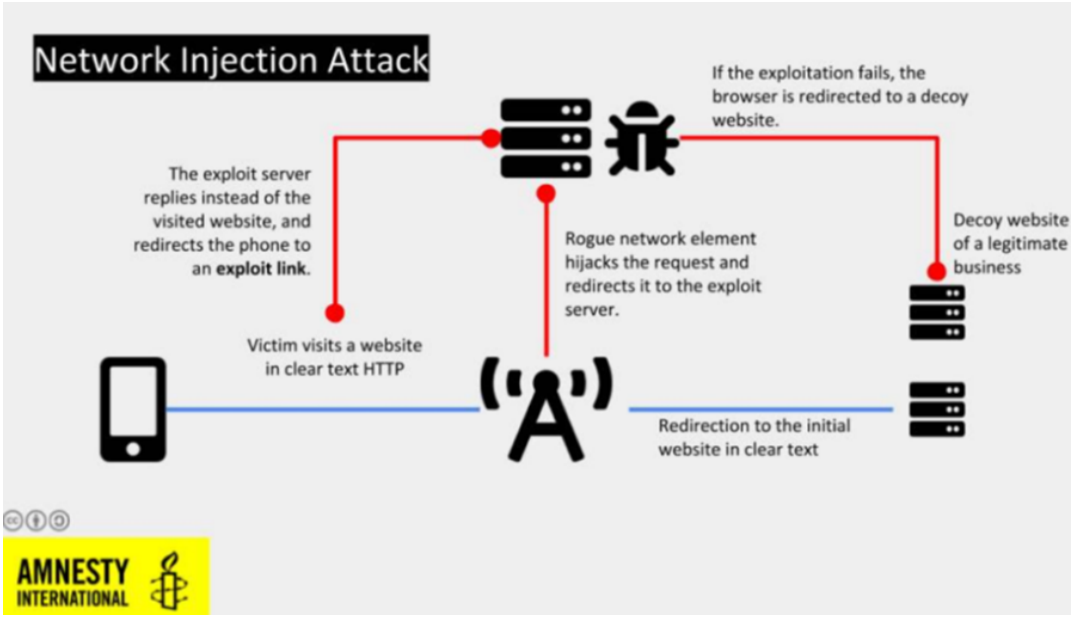

Figure 2: A diagrammatic representation of how a Network Injection Attack occurs[15]

- Perhaps one of the most widely recognized examples of an SQL injection would be when a hacker uses a web form or comment field to insert an SQL command. Carrying this to the extreme, the application will surreptitiously send the attacker's data to the database and execute any SQL command that is embedded in the query. Most web applications use

[15] "How Journalists Are Coping with a Heightened Surveillance Threat." Gijn.org, www.gijn.org/stories/how-journalists-are-coping-with-a-heightened-surveillance-threat/.

databases constructed with Structured Query Language (SQL), so SQL injection can be a very serious security problem.

- NoSQL attacks are a new kind of attack that does not focus on the databases whose data is not in the form of a relation structure. In a code injection, the attacker goes on to inject codes in an application with vulnerabilities. The web server executes this malicious code as if it were part of the application. The injection of operating system commands occurs when an attacker exploits command injection to enter the commands that the operating system must execute. This leaves the system open to potential takeover or exfiltration of OS data by the assault.
- Lightweight Directory Access Protocol injections involve the attacker inputting special characters, which modify LDAP queries. A system becomes vulnerable if it utilizes uncleared LDAP query. Since the LDAP servers can potentially house the identities and credentials of every user within a business, these kinds of attacks are very dangerous.
- In XXE Injection, an attack is performed via specially crafted XML documents. In contrast with other attack vectors, this vector exploits unvalidated user inputs and not vulnerabilities of the legacy XML parsers. It is possible to traverse pathways, execute remote code and conduct server-side request forgery by means of XML documents.
- An XSS injection is a case where an attacker provides a malicious string of JavaScript. The code, after execution by the target's browser, grants the attacker the ability to conduct a variety of harmful actions, such as taking over a user's session or redirecting them to a malicious website by stealing session cookies.

The impact of Cybersecurity Threats to Journalists

Digital and physical threats to journalists are connected. For instance, the use of spyware has been linked to hundreds of acts of physical violence around the world. In particular, human rights organizations and cybersecurity experts have expressed concerns about the use of spyware largely developed by companies in Europe, the Middle East and the U.S. — including NSO Group's 'Pegasus' and QuaDream's 'Reign' — being used in dozens of countries around the world, especially in Latin America. In addition to raising safety and psychosocial concerns, digital security threats also damage trust in the news media. In an attention economy, cyberattacks can eliminate entire business models and push audiences away by slowing or crashing websites.[16]Journalists who report on equality and issues of minority-group belonging

[16] "Journalists & Cyber Threats." Center for News, Technology & Innovation, www.innovating.news/article/journalists-cyber-threats/.

also suffer disproportionate attacks, with many of these assaults remaining unreported and unrecorded by established monitoring systems. Online assault takes the primary forms of threats and insults via social media but also includes impersonation of an account, doxing, electronic stalking, and surveillance, along with non-consensual photographs and violent threats.

Major parties involved

Bangladesh

In August 2023, the Bangladesh government approved the final draft of its Cyber Security Act (CSA), developed to tone down the country's Digital Security Act (DSA) that was previously passed, amid global criticism and allegedly remove vaguely worded provisions that can easily be abused to restrict press freedom. Human rights organizations have argued that the CSA retains most provisions used to curtail free expression and privacy[17]. Therefore, this indicates that in order to limit cybersecurity threats to journalists, policies must be completely transparent and clear.

United States of America

In early 2023, the Biden administration released a wide-ranging cybersecurity strategy aiming to bolster protections against cyberattacks. More specifically, the administration has taken action to counter spyware abuses, including announcing a multi-country collaboration to control the proliferation of these technologies and signing an executive order to prohibit U.S. governmental use of commercial spyware. Meanwhile, bipartisan U.S. House and Senate bills (the PRESS Act) have been reintroduced with the aim of shielding journalists' communication records and data. The act would limit the government's ability to require journalists to disclose data that could identify their sources, with limited exceptions for terrorism and the imminent threat of violence. The PRESS Act has largely been applauded by experts as creating strong protections for independent journalism[18].

Norway

Norway's strategy looks forward to the establishment of robust cybersecurity in various sectors that include the area of media and journalism. The Norwegian government organizes periodic training and awareness programs specifically tailored for journalists by establishing a National Cyber Security Centre in Norway, NorCERT. These programs entail secure communication practices, an understanding of

---

[17] "Bangladesh: Government Enacts Cybersecurity Act 2023." DataGuidance, 4 Mar. 2024, www.dataguidance.com/news/bangladesh-government-enacts-cybersecurity-act-2023#:~:text=Further%2C%20the%20Cybersecurity%20Act%20provides.

[18] "Country in Focus: United States - Center for News, Technology & Innovation." Center for News, Technology & Innovation, 3 Apr. 2024, www.innovating.news/article/country-in-focus-united-states/.

phishing attempts, and ways to use encryption tools effectively in protecting sensitive data. NorCERT provides a rapid-response service to information organizations in case of a cyberattack and has follow-ups to reduce damage and restore services[19]. They also work closely with their international partners regarding threat intelligence sharing. In sum, Norway had been quite successful with its comprehensive approach to preventive education and responsive support. This high degree of cooperation among public and private sectors—including media companies—has greatly reduced the problem of cyber-attacks against Norwegian journalists. Although this policy has been effective for the security of national media, both the international scope of journalism and that of the internet more generally imply that Norwegian journalists abroad are highly vulnerable. A domestic approach of the strategy does little to mitigate these risks abroad.

Council of Europe

In September 2023, the Parliamentary Assembly of the Council of Europe's Committee on Legal Affairs and Human Rights released a spyware report, citing "mounting evidence" that member-states have used spyware for illegitimate purposes and asking five countries to investigate abuses. The committee also requested information from Israel on how it ensures Pegasus spyware isn't acquired to violate human rights. The Council has called on member-states to establish spyware oversight structures. This was an effective solution as it covered international threats and ensured that all such threats were carefully monitored and examined, thereby improving accountability[20].

UNESCO

The UNESCO report Threats that Silence: Trends in the Safety of Journalists spotlights the methods that criminals use to interfere with press freedom, including hacking (such as to steal confidential data) and digital attacks (one example is DDoS attacks to overwhelm a site with traffic). This publicly available report increases awareness about the issue of cybersecurity attacks by providing publicly available information on how to combat them[21]. Furthermore, the UNESCO International Programme for the Development of Communication's Journalists Safety Indicators were designed with the aim of assessing the level of safety of journalists and to assess ways in which the governments and institutions react to crimes against them. These indicators provide a conceptual framework for an estimation of the risks that surround journalists, including

---

[19] "NorCERT." The IT Law Wiki, Fandom, Inc., 2024, www.itlaw.fandom.com/wiki/NorCERT.

[20] "Journalists & Cyber Threats." Center for News, Technology & Innovation, www.innovating.news/article/journalists-cyber-threats/.

[21] "The World Urban Forum 12." Www.climate-Chance.org, www.climate-chance.org/en/event-calendar/world-urban-forum/.

cyber threats and how far protection measures are effective[22]. The JSI has been instrumental in pinpointing specific issues that impact journalist safety, including in countries like Guatemala, Kenya, Nepal, and Pakistan. It has managed to frame in clearer terms the structural problems that need to be overcome in the name of protecting journalists. As a successful problem-diagnostic instrument, the JSI has had its difficulties with actually moving governments to act upon its findings. In many cases, there remains a lack of political will to act upon the concerns raised by the JSI, which perpetuates vulnerability for journalists.

Timeline of Key Events

14 December 2021	The UN Conference on Trade and Development found that 80% of countries had enacted cybercrime legislation[23].
14 September 2023	The Parliamentary Assembly of the Council of Europe's Committee on Legal Affairs and Human Rights released a spyware report.
18 September 2023	The Bangladesh government approved the final draft of its Cyber Security Act (CSA).
12 March 2024	The EU Cyber Resilience Act is adopted which provides cybersecurity regulations[24].

Previous attempts to solve the issue

United Nations Cybercrime Treaty Negotiations

The United Nations is currently leading negotiations to develop a comprehensive, all-inclusive global cybercrime treaty. The objective is to create a standard international convention on cybercrime, an increasingly global issue. The negotiation process has been very technical and political, with debates focusing primarily on defining what cybercrime is, what the parameters of the treaty are to be, and how the treaty is to reach the right balance of security concerns and

---

[22] "Journalists & Cyber Threats." Center for News, Technology & Innovation, www.innovating.news/article/journalists-cyber-threats/.

[23] UNCTAD. "Cybercrime Legislation Worldwide | UNCTAD." Unctad.org, 14 Dec. 2021, www.unctad.org/page/cybercrime-legislation-worldwide.

[24] "EU Cyber Resilience Act." Shaping Europe's Digital Future, 2020, www.digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act#:~:text=The%20Cyber%20Resilience%20Act%20is.

human rights[25]. The lengthy negotiations have served to raise global awareness of the need for an international legal framework on cybercrime. They have provided a forum for debate among countries with disparate views on digital governance. One of the major concerns is that the definition of cybercrime could be so broad or vague that autocratic regimes would use it to target journalists and stifle freedom of expression. This risk has had questions raised regarding the implications of the treaty on human rights, especially the safety of journalists, who might get attacked in the disguise of fighting cybercrime.

United Nations Secretary-General's Reports on the Safety of Journalists, 2014, 2015, 2017

There have been a number of reports generated by the United Nations Secretary-General, targeting the question of the safety of journalists and the problem of impunity, which relates to crimes conducted against such journalists. The reports have shed light on the dangers in which journalists live and even on the risks of digital threats. Furthermore, the reports have argued for the dissemination of awareness on specific risks that journalists face in connection with poor cybersecurity. Along the same vein, they provide the foundation for further UN actions and resolutions designed to enhance the safety of journalists. While these reports have been useful in bringing issues to the fore, very little has materialized in terms of policy change. The recommendations made in the reports were often slow to translate into concrete actions by member states, particularly in regions where press freedom is already under threat[26].

Work by Citizen Lab, The Committee to Protect Journalists, and Forbidden Stories

Organizations such as the University of Toronto's Citizen Lab, the Committee to Protect Journalists, and Forbidden Stories have documented myriad cases of spyware and digital surveillance being used against journalists. They have focused mainly on the dangers of companies like NSO Group, whose spyware has put journalists around the world under surveillance and in some cases appears to have helped jail, or potentially threaten, reporters or their sources into silence. Such groups have been conspicuously successful in bringing to the fore the digital surveillance tools about which journalists were either being or were already under surveillance, with the arrests gaining international focus. Their work has gained legal ground in suits, policy changes, and increased scrutiny of companies involved in producing and selling spyware. This is often streamlined by the lack of enforceable international regulations against the

---

[25] UN News. “Global Cybercrime Treaty: A Delicate Balance between Security and Human Rights | | UN News.” News.un.org, 25 Feb. 2024, www.news.un.org/en/interview/2024/02/1146772.

[26] “Amid Growing Cybersecurity Threats, Rule of Law in Digital Sphere Critical to Ensure New Technologies Are Used for Common Good, Secretary-General Tells Security Council | Meetings Coverage and Press Releases.” Press.un.org, www.press.un.org/en/2024/sgsm22280.doc.htm.

abuse of surveillance technology. While there has been a sense of awareness derived from this period, arguably more concrete actions towards stopping the practices are needed, first and foremost in countries with weak legal protection for journalists[27].

Amnesty Tech and Digital Forensic Efforts

Amnesty Tech has been at the core of digital forensics, looking into cyber attacks against journalists and giving them the opportunities and capacity to protect themselves online, be it malware analysis, infrastructure attribution, or building journalist resources for improved cybersecurity. Their work so far has been crucially important in documenting digital threats and providing journalists with actionable information to defend against them', which has helped in the reduction of some attacks and protection of journalists in high-risk environments. For all that, the scale of the problem is still overwhelming. Many news organizations, especially in resource-poor settings, lack the capacity to implement the advanced cybersecurity measures recommended by Amnesty Tech[28]. In addition, across the globe, the pace at which surveillance technology is being rolled out surpasses efforts to protect journalists.

Global Programme on Cybercrime by the United Nations Office on Drugs and Crime

The UNODC's Global Programme on Cybercrime aims to assist member states in their efforts to combat cybercrime, focusing on capacity building, technical assistance, and legal frameworks. It is designed to acknowledge the kind of threats journalists face and to create a mainstream flow of freedom of expression into larger cybersecurity endeavours[29]. The program not only enabled international cooperation against cybercrime but also increased the technical capacities of many countries' law enforcement agencies. It has also contributed to the development of international standards that consider the rights of journalists. One of the biggest challenges involves the discrepancies on how to balance security concerns and human rights, leading to extremely non-uniform implementations on a country-to-country basis. It sometimes allows countries to use cybercrime laws to imprison journalists instead of protecting them.

---

[27] “Journalists & Cyber Threats.” Center for News, Technology & Innovation, www.innovating.news/article/journalists-cyber-threats/.

[28] “NSO Spyware Used against Moroccan Journalist Days after Company Pledged to Respect Human Rights.” Amnesty International, 22 June 2020, www.amnesty.org/en/latest/news/2020/06/nso-spyware-used-against-moroccan-journalist/.

[29] “United Nations Office on Drugs and Crime (UNODC) - the GFCE.” The GFCE, 30 Jan. 2024, www.thegfce.org/member-and-partner/united-nations-office-on-drugs-and-crime-unodc/#:~:text=Partner%20Description%3A%20The%20UNODC%20Global.

Cyber Resilience Act (European Union)

Coming into force in 2022 and eventually adopted by 2024, the EU Cyber Resilience Act is but one way the European Union tightens its belt around the globe for cybersecurity regulations on commercial spyware use and other digital threats. Above all, the Act deals with the dangers to human rights and personal privacy by limiting the use of such spyware by police and obligations to investigate abuses[30]. This is, therefore, one major leap in protecting journalists and other vulnerable groups from cyber risks within the EU. Should it really work, other regions will follow such regulations about the use of surveillance technology. The Act has been hailed as something commendable that may safeguard the user populations, but success can only be achieved after rigorous enforcement and cooperation from all EU member states. There is also a question of how well these regulations can be enforced, especially in countries where strong surveillance is conducted.

Project Galileo

Project Galileo, run by cybersecurity company Cloudflare, provides at-risk organizations, including, media houses, with free protection against cyber-attacks. So far, and it has enrolled organizations in 111 countries, with one of the key priorities being protecting journalists and civil society groups from DDoS and other cyber aggression. Project Galileo has been an enormous success in providing vital cybersecurity services to under-resourced media organizations and NGOs[31]. It has shielded many such outlets from cyberattacks that might have easily silenced them, particularly from the stress of conflict zones and in countries with authoritarian regimes. But that was the strength—and weakness—of a project that relies on private initiative and financing. Key concerns are towards the long-term sustainability of such projects and their capability to scale up to meet increasing demand.

Possible solutions

Collaboration Among Stakeholders

Digital security threats facing journalists are not isolated issues that can be easily addressed by individual newsrooms, especially those in hostile environments or operating in exile. There is a need to rope in collaborative efforts from policymakers, technology platforms, researchers, and

---

[30] “EU Cyber Resilience Act | Shaping Europe’s Digital Future.” Digital-Strategy.ec.europa.eu, www.digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

[31] McLaughlin, Jenna. “Why Cyberattack Cases against Journalists Are Increasing.” Ideastream Public Media, Ideastream Public Media, 24 June 2024, www.ideastream.org/2024-06-24/why-cyberattack-cases-against-journalists-are-increasing.

organizations operating in the sphere of civil society. For example, technology companies can establish and enforce safeguards of human rights and privacy; publishers can do so in a proactive way in cyber education, safety support, and sharing of best practices within the industry; and researchers and civil society in putting a spotlight on trends, risks, and potential solutions by means of data collection and analysis. The weakness in this solution is that adequate collaboration is often limited due to competing interests. For example, balancing difficult state demands that can sometimes require a platform to provide private user data, which may lead to power abuses. Furthermore, every stakeholder differs in commitment and resources, so it is very hard to collaborate consistently and effectively in these ways. Without global evidence and communication on these practices, such efforts may not have the impact necessary to fully address these threats.

Governmental and Legislative Measures

Members of legislatures can protect journalists by developing laws to protect freedom of expression, including privacy rights and encryption protections. Some of the measures through which governments can do this are having open legislative processes in relation to cybercrime and cybersecurity legislation, including the voices of media, journalists, and civil society from the start. Specific laws need also to be designed for journalists against forced disclosure of sources or private data except under strictly defined legal circumstances. Governments should also facilitate cooperation between law enforcement and media bodies to underscore better identification and addressing of threats, in particular, those creating personal protection for journalists at risk. Despite such measures, the wording of many cybercrime laws is still very broad and vague, potentially targeting independent press and suppressing free expression. A lack of definitional clarity as to who is a journalist may further lead to fitful legal protections, especially in cases of freelancers, citizen journalists, or reporters working in war zones. Besides, such policies are executed very differently in different countries, making universal protection hard to accomplish.

Platform-Level Initiatives

Technology platforms can help safeguard journalists by putting in stringent human rights and privacy safeguards. This would have included encryption of channels of communications, the offering of secure mechanisms of sharing information, and resisting state demands that violate user privacy. Sure enough, the platforms can work far more closely with cybersecurity experts in ensuring their services do not get turned for ill use. More so, they will also work with specialized organizations handling threats against journalists to identify and mitigate online harassment and threats of violence.

Publisher and Media Organization Efforts

Enhancement of cyber-education, safety support, and experience-sharing across the industry can work wonders for publishers and media organizations toward digital security. Additional layers of cybersecurity solutions, such as application security, network security, and endpoint security, further improve overall safety. Other very important measures include providing training[32] in cybersecurity best practices for journalists and equipping them with various tools such as VPNs and encrypted channels of communication[33]. Despite this, little priority, if not at all, is placed on digital security as compared to physical security by publishers. Conflicting priorities between the editorial teams and IT departments on measures of security—such as the use of VPNs—also complicate the implementation of effective digital security measures within newsrooms. Many journalists also treat security as an individual issue rather than a collective responsibility; hence, the application of security measures is patchy within newsrooms.

Research and Contributions of Civil Society

Researchers and civil societies are equally important in the understanding and fending off digital threats against journalists. Those groups can provide studies and give data on trends, risks, and potential solutions that can be used for the betterment of policies and platform initiatives. Civil society can advocate for the rights of journalists while providing security tools which are easy to use, especially for journalists through collaboration with cybersecurity experts[34]. One of the potential limitations is related to communication: researchers, civil society, and journalists are really not that effective in communication all the time; hence, some gaps in knowledge and dissemination of best practices exist. Unless made more coordinated, these efforts may not suffice against the complex and fast-evolving digital threats to the lives of journalists.

Further reading

https://press.un.org/en/2024/sc15738.doc.htm

www.innovating.news/article/journalists-cyber-threats/.

https://ec.europa.eu/commission/presscorner/detail/en/ip_21_4632

---

[32] Marina. “Protecting Journalists in High Cyber Risk.” GCA | Global Cyber Alliance | Working to Eradicate Cyber Risk, GCA | Global Cyber Alliance | Working to Eradicate Cyber Risk, 30 Oct. 2023, www.globalcyberalliance.org/protecting-journalists-cyber-risk/.

[33] “Journalists & Cyber Threats.” Center for News, Technology & Innovation, www.innovating.news/article/journalists-cyber-threats/.

[34] Mitchell, Amy S. “Journalists Need to Be Protected from Cyber Threats | TechPolicy.Press.” Tech Policy Press, 8 Jan. 2024, www.techpolicy.press/journalists-need-to-be-protected-from-cyber-threats/.

Bibliography

Amid Growing Cybersecurity Threats, Rule of Law in Digital Sphere Critical to Ensure New Technologies Are Used for Common Good, Secretary-General Tells Security Council | Meetings Coverage and Press Releases. United Nations, www.press.un.org/en/2024/sgsm22280.doc.htm.

Bangladesh: Government Enacts Cybersecurity Act 2023. DataGuidance, 4 Mar. 2024, www.dataguidance.com/news/bangladesh-government-enacts-cybersecurity-act-2023#:~:text=Further%2C%20the%20Cybersecurity%20Act%20provides.

Coker, James. “Cyber-Attacks in the Media Industry Making Headlines.” Infosecurity Magazine, 13 Mar. 2023, www.infosecurity-magazine.com/news-features/cyber-attacks-media-industry/.

Country in Focus: United States - Center for News, Technology & Innovation. Center for News, Technology & Innovation, 3 Apr. 2024, www.innovating.news/article/country-in-focus-united-states/.

Cyber Attack - Glossary | CSRC. NIST Computer Security Resource Center, www.csrc.nist.gov/glossary/term/cyber_attack#:~:text=An%20attempt%20to%20gain%20unauthorized.

Digital Breakthroughs Must Serve Betterment of People, Planet, Speakers Tell Security Council during Day-Long Debate on Evolving Cyberspace Threats | Meetings Coverage and Press Releases. United Nations, www.press.un.org/en/2024/sc15738.doc.htm.

EU Cyber Resilience Act. Shaping Europe’s Digital Future, 2020, www.digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act#:~:text=The%20Cyber%20Resilience%20Act%20is.

EU Cyber Resilience Act | Shaping Europe’s Digital Future. Digital-Strategy.ec.europa.eu, www.digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

Imperva. “Cyber Security Threats | Types & Sources | Imperva.” Imperva, 2022, www.imperva.com/learn/application-security/cyber-security-threats/.

How Journalists Are Coping with a Heightened Surveillance Threat. Gijn.org, www.gijn.org/stories/how-journalists-are-coping-with-a-heightened-surveillance-threat/.

Journalists & Cyber Threats. Center for News, Technology & Innovation, www.innovating.news/article/journalists-cyber-threats/.

Journalists & Online Abuse. Center for News, Technology & Innovation, 22 July 2024, www.innovating.news/article/journalists-online-abuse/.

Mitchell, Amy S. “Journalists Need to Be Protected from Cyber Threats | TechPolicy.Press.” Tech Policy Press, 8 Jan. 2024, www.techpolicy.press/journalists-need-to-be-protected-from-cyber-threats/.

McLaughlin, Jenna. “Why Cyberattack Cases against Journalists Are Increasing.” Ideastream Public Media, 24 June 2024, www.ideastream.org/2024-06-24/why-cyberattack-cases-against-journalists-are-increasing.

Marina. “Protecting Journalists in High Cyber Risk.” GCA | Global Cyber Alliance | Working to Eradicate Cyber Risk, 30 Oct. 2023, www.globalcyberalliance.org/protecting-journalists-cyber-risk/.

NSO Spyware Used against Moroccan Journalist Days after Company Pledged to Respect Human Rights. Amnesty International, 22 June 2020, www.amnesty.org/en/latest/news/2020/06/nso-spyware-used-against-moroccan-journalist/.

NorCERT. The IT Law Wiki, Fandom, Inc., 2024, www.itlaw.fandom.com/wiki/NorCERT.

Press Corner. European Commission, www.ec.europa.eu/commission/presscorner/detail/en/ip_21_4632.

Rosencrance, Linda. “What Is Software? Definition, Types and Examples.” SearchAppArchitecture, Mar. 2021, www.techtarget.com/searchapparchitecture/definition/software#:~:text=Software%20is%20a%20set%20of.

Shere, Anjuli, et al. “How the Internet of Things Poses a Threat to Journalists.” The Journalist’s Resource, 1 Nov. 2021, www.journalistsresource.org/home/how-the-internet-of-things-poses-a-threat-to-journalists/.

The Deluge of Digital Attacks against Journalists. The Cloudflare Blog, 3 May 2022, www.blog.cloudflare.com/the-deluge-of-digital-attacks-against-journalists.

The World Urban Forum 12. Climate Chance, www.climate-chance.org/en/event-calendar/world-urban-forum/.

UN News. “Global Cybercrime Treaty: A Delicate Balance between Security and Human Rights | | UN News.” UN News, 25 Feb. 2024, www.news.un.org/en/interview/2024/02/1146772.

UNCTAD. “Cybercrime Legislation Worldwide | UNCTAD.” UNCTAD, 14 Dec. 2021, www.unctad.org/page/cybercrime-legislation-worldwide.

United Nations Office on Drugs and Crime (UNODC) - the GFCE. The GFCE, 30 Jan. 2024, www.thegfce.org/member-and-partner/united-nations-office-on-drugs-and-crime-unodc/#:~:text=Partner%20Description%3A%20The%20UNODC%20Global.

LmunA 2024

What Is Spoofing? Cisco, www.cisco.com/c/en/us/products/security/email-security/what-is-spoofing.html#:~:text=Spoofing%20is%20a%20type%20of.

Why Journalism Needs Information Security. Reuters Institute for the Study of Journalism, 2020, www.reutersinstitute.politics.ox.ac.uk/calendar/why-journalism-needs-information-security.