CORA Cork Open Research Archive
Cartlann Taighde Oscailte Chorcaí

Title	Insecure software on a fragmenting internet
Authors	Ryan, Ita;Roedig, Utz;Stol, Klaas-Jan
Publication date	2022-04-25
Original Citation	Ryan, I., Roedig, U. and Stol, K.-J. (2022) 'Insecure software on a fragmenting internet', 2022 Cyber Research Conference - Ireland (Cyber-RCI), Galway, Ireland, 25 April 2022, pp. 1-9. https://doi.org/10.1109/Cyber-RCI55324.2022.10032675
Type of publication	Conference item
Link to publisher's version	https://cyber-rci.com/2022 - 10.1109/Cyber-RCI55324.2022.10032675
Rights	© 2022
Download date	2026-11-16 11:03:33
Item downloaded from	https://hdl.handle.net/10468/13668

UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Insecure Software on a Fragmenting Internet

Ita Ryan
School of Computer Science and IT
University College Cork
Cork, Ireland
ita.ryan@cs.ucc.ie

Utz Roedig
School of Computer Science and IT
University College Cork
Cork, Ireland
utz.roedig@cs.ucc.ie

Klaas-Jan Stol
Lero, School of Computer Science
University College Cork
Cork, Ireland
k.stol@ucc.ie

***Abstract*—Global geopolitical forces are pushing much of the world towards Internet nationalism, threatening to turn the Internet into a 'Splinternet.' In this paper we argue that the crisis in software security will exacerbate this trend. We examine existing moves towards Internet fragmentation on multiple levels. We discuss current trends in online crime, espionage, and warfare. We look at the role of software vulnerabilities, discussing how the prevalence of software security issues could propel nations further apart. We argue that there is an urgent need for a 'zero tolerance' attitude to software security issues, and discuss what is needed to create this.**

***Index Terms*—Cybersecurity, software security, Internet nationalism, Splinternet**

I. Introduction

With its elegant protocols and built-in redundancy, the Internet is inherently global in nature. Nevertheless, it is not immune to geopolitical forces. Inter-country fragmentation is happening on several different levels, and has been referred to as the 'Splinternet' [1].

Ubiquitous access to the Internet means that software flaws can be exploited remotely from anywhere, with local law enforcement having no jurisdiction in the country from which a crime was committed. Thus, the Internet facilitates previously unimaginable scenarios like the May 2021 ransomware attack on the Irish Health Service Executive [2]. Similarly, espionage, sabotage, and cyberwarfare can be conducted remotely, providing hostile forces with unprecedented access.

Secure software is a core cybersecurity concern. While firewalls, anti-virus tools, network segmentation, and other tools and strategies are deployed to protect digital assets, software defects and design flaws can provide attackers with a back door. It is impossible to prove the security of non-trivial software. Indeed, severe implementation flaws have been found in firewalls [3], anti-virus tools [4] and network segmentation tools [5] themselves.

The number of newly reported software vulnerabilities increases each year [6]. Efforts to tackle software security issues are haphazard. Until very recently there was little government guidance, and organisational software security drives in unregulated industries are entirely voluntary. While critical domains use regulations often based on the U.S. National Institute of Standards and Technology (NIST) guidelines, these guidelines are rather heavy-weight, and thus unsuitable for most organisations. We argue that a rapid escalation of effort in eliminating software vulnerabilities is needed. Otherwise, exploitation will continue to increase, exacerbating the trend towards Internet nationalism. The vulnerability of military and critical infrastructure and of nuclear control software to remote exploitation will be seen as too much of a risk.

Previously, Claessen [7] discussed how the understanding of cyberspace as a military as well as civilian domain has led to increasing attempts to impose state sovereignty on the Internet, with particular reference to the different approaches adopted by Russia and the European Union (EU). Hoffman looked at how the new technical standards proposed by China could lead to Internet fragmentation [1]. In this paper, we contribute to this line of work by examining contemporary pressures on a cohesive Internet, explore the forces that are driving the Internet to fragment, and consider how untamed software security risk adds to those pressures. We advocate for a new culture of software insecurity intolerance.

In Section II we look at drivers towards Internet nationalism and ways in which countries are currently uncoupling from a cohesive global Internet. In Section III we discuss large scale security issues that the Internet facilitates. In Section IV we examine how software vulnerabilities impact on cybersecurity. In Section V we discuss approaches to reducing software vulnerabilities, and some exacerbating factors. The conclusion in Section VI discusses possible global consequences of a failure to improve software security.

II. Internet Nationalism

Internet fragmentation is an existing phenomenon driven by perceived national interest and facilitated by design choices on different Internet layers. We first discuss the different layers in which changes are happening. We then briefly discuss how some countries are diverging on multiple levels.

A. OSI Model Layer 1: Physical

Approximately 95% of global Internet traffic travels through undersea fibre-optic cables, which comprise the Internet's backbone [8]. Cables are increasingly perceived as relevant to geopolitical tensions [9]. Russian naval exercises off the Irish coast in January 2022 focused minds on the vulnerability of transatlantic communications cables, damage to which would severely impair Irish and European Internet connectivity [10]. Underlining the fragility of the world's Internet connectivity, in January 2022 Tonga's external communications were almost

completely cut off after a volcanic explosion severed the single undersea cable connecting it to Fiji [8].

Russia recently decreed that its transnational cables must be registered with a central authority [11]. Data on transnational cables is already collated and made public in the U.S. [12]. U.S. researchers recently mapped crucial internal cables in a project funded by the Dept. of Homeland Security [13].

There is concern about espionage via physical cable access [14], with China-funded cables increasingly regarded with suspicion [15]. The U.S. Department of Justice (DoJ), in 2020, objected on national security grounds to a new undersea cable connecting the U.S. to Hong Kong [16].

B. OSI Model Layer 2: Data Link

The U.S. have banned use of Chinese company Huawei's technology in 5G networks, citing security concerns [17]. Four other Chinese tech companies have also been deemed security threats by the U.S. Federal Communications Commission (FCC) [18]. Russia mandates use of local technology for key Internet controls [11]. As each country moves to using only local suppliers, commonality declines and the feasibility of standards and protocols diverging increases.

C. OSI Model Layer 3: Network

Communication between networks is often done via Internet Exchange Points (IXPs) where multiple network endpoints are located in close proximity, using Border Gateway Protocol (BGP) records to move traffic directly between networks. This may be done for example to avoid transit fees [19]. BGP can be used to prevent a nation's Internet traffic from travelling through another nation's territory. Russia has directed that Internet traffic should only be directed through approved IXPs registered with Roskomnadzor [7]. This policy is likely to keep Russian Internet traffic within the country.

Because BGP is the protocol that allows networks to find destinations, it can also be used for censorship. Pakistan accidentally propagated an incorrect YouTube destination to the global Internet when it banned YouTube in 2008 [20]. Ververis et al. [21] found that BGP configuration is one of the most widely-used tools for Internet censorship. Limonier et al. found that, over the six years prior to 2020, Internet traffic from disputed Donbas in Ukraine shifted to being routed almost entirely through Russia [22]. They concluded that routing can reflect geopolitical concerns.

D. OSI Model Layer 4: Transport

All Internet traffic currently uses TCP/IP. While the transition from IPV4 to IPV6 brings its own fragmentation concerns [23], China has proposed a 'decentralised Internet' model and associated entirely new protocol named New IP. It argues that the 50-year-old IP protocol is creaking under today's massive Internet use and new communication needs for technologies like virtual and augmented reality [24]. New IP facilitates centralised surveillance and control of the Internet, and is seen by some as entailing the loss of individual freedom to the state [1]. It is suggested that the protocol will not be adopted by the U.S. or its allies and that this could lead to a fragmentation into at least two separate versions of the Internet, with different countries or blocs using their own protocols. Hoffman et al. [1] note that, although involvement in Internet protocol standards committees is resource-intensive and expensive, nations should participate in order to ensure that their values are reflected.

E. Data, Applications and Access

China, Russia, and other states require data pertaining to their citizens to be stored within their borders [25]. The EU only allows data to be held overseas if certain privacy and protection guarantees are followed. Data localisation allows states to ensure that their data remains within their jurisdiction, but it also contributes to fragmentation.

Many countries have banned or restricted other countries' websites and applications for reasons of censorship, privacy or national security. For example, China's 'Great Firewall' prevents the use of Twitter, Facebook, Google, Signal and numerous other applications [26]. In 2020, India banned over 200 Chinese apps including Baidu, WeChat and Alipay, citing national security and surveillance concerns amid escalating border tensions [27]. Russia's February 2022 invasion of Ukraine was swiftly followed by a ban on Instagram, Facebook and other sites due to 'extremist activities.' In March 2022, the FCC added Russian anti-virus organisation Kaspersky, already banned from U.S. government networks, to its list of firms posing a security threat [28].

Governments may use strategies to control the flow of information over the Internet [29], often to limit foreign content. In a 2020 global, longitudinal study of Internet censorship, Niaki et al. [30] found the most censorship overall in Iran, South Korea, Saudi Arabia, Kenya, and India. India is the world's largest democracy, a reminder that censorship is not the sole preserve of authoritarian regimes. Conservative countries may resist open access to pornographic or gambling sites, seeing these as conflicting with national values.

Removal of Internet access is a favourite tool of oppressive regimes in times of turmoil. For example, most Internet access was lost for three days during the 2016 general election in Uganda [31]. In Belarus, where all Internet access is government controlled, there was a 61-hour Internet blackout during protests against a disputed Presidential election result in August 2020 [32]. In Myanmar in February 2021, new cybersecurity laws were introduced allowing mass censorship and surveillance after a military coup. In January 2022, Kazakhstan was subject to an Internet blackout amid anti-government protests about fuel charge hikes [33]. Those are a few examples among many; the Access Now activist group estimated that there were at least 155 Internet shutdowns in 29 countries in 2020 alone (https://www.accessnow.org/).

F. Multi-Level Divergence

China's Internet is a model for all nations, like Russia, that want to be able to disconnect from the global Internet at will. It has no foreign telecommunications companies within its borders. External connections are made via cables that pass

TABLE I
ENISA CYBER CRIME ACTORS & MOST COMMON ACTIVITIES 2020-2021

Level	Description
State-sponsored actors	Malware Espionage Supply chain compromise Disinformation\misinformation Cybercrime for monetary gain Sabotage (targeting of Industrial Control System (ICS)s) Cyber arms race
Cybercriminals	Ransomware Cryptojacking Malware Cybercrime-as-a-service DDoS, Web Attacks
Hacker-for-hire actors	Access-as-a-Service
Hacktivists	DDoS Sensitive data release Account takeovers

through the 'Great Firewall,' leave China, and connect with external IXPs on foreign soil [34].

Having banned most U.S. apps, China has very successful social media apps of its own. Chinese government organisations were ordered to remove foreign hardware and software from their offices by the end of 2022 in a 2019 edict [35]. This move away from reliance on computers and software developed by the U.S. and its allies, along with the Intranet-like nature of China's Internet, its use of the 'Great Firewall' and its drive to replace IP with New IP show that China is splitting from the global Internet on multiple levels.

Russia has been attempting to emulate China and modify its Internet (the 'RuNet') to remove dependence on external connections at every level. For example, in 2017 the Russian Security Council launched a process for developing a parallel DNS service [36]. A 2019 law mandated installation of local apps on devices sold in Russia [37]. Successful tests of RuNet independence were reported in 2019 and 2021 [38].

Subsequent to the Russian invasion of Ukraine in February 2022, many foreign service providers withdrew from the Russian market [39]. Others were banned by Russia. The Ukrainian representative at ICANN requested that top-level Russian domains and certificates be revoked by ICANN [40]. ICANN refused this unprecedented request. In early March 2022, the rumour that Russia would disconnect itself entirely from the global Internet on March 11, apparently based on a Kremlin document on preparing for separation, was widespread [41]. Some commentators suggested that this would presage an all-out cyberattack on the U.S., or the cutting of transatlantic cables by Russia. Calls for Russia to be disconnected from the Internet, and rumours that it will disconnect itself, are still circulating at time of writing in April 2022.

III. SECURITY ISSUES FOR A GLOBAL INTERNET

Metcalfe's law states that the value of a communications network is proportional to the square of the number of connected users of the system [50]. However, it has been shown that an increase in the number of connected users also increases risk, which in turn diminishes value [38]. In this paper we argue that the uncertainty and fragility caused by widespread insecure software is likely to add further pressure to a global Internet infrastructure that is already fragmenting. We base this argument on the fact that insecure software facilitates crime, espionage and sabotage across borders. In this section we discuss the top crimes and threats from the Threat Landscape report issued by The European Union Agency for Cybersecurity (ENISA) [42], which covers the year prior to July 2021. Published in October 2021, the report lists the main threats encountered and defines four categories of threat actor. Like the ENISA report, we do not consider localised issues such as those related to intimate partner abuse and cyberbullying, because those very real risks are not primarily international. Having discussed threats defined by ENISA, we add cyber patriotism and cyberwarfare.

A. Threat actors in the ENISA report

The ENISA report defines four different threat actors.

1) State-Sponsored Actors: The report (see Table I) describes a rise in cyberespionage related to Covid-19, with state actors observed searching for information on national Covid-19 responses and treatment. Healthcare and medical research sources were targeted. Supply-chain compromises were significant, in particular the highly sophisticated SolarWinds SunBurst breach [43]. State actors were observed engaging in money-making activities such as cryptojacking, perhaps partially to disguise breaches as cybercrime.

Both defenders and state actors raised their game in the reporting period, with numerous joint declarations and legal stratagems. State actors showed increasing levels of sophistication. 'False flags' were sometimes used to muddy attribution, and hack-and-leak campaigns were used for strategic gains.

2) Cybercriminals: Covid-19 was used by cybercriminals in multiple phishing campaigns preying on concern about the virus. The report notes increased collaboration and professionalism, a move to the cloud and an increasing tendency to attack critical infrastructure. The report mentions the 'Cybercrime-as-a-Service' trend, wherein services for cybercrime are commoditised and broken down; it is possible to purchase access to victim servers from one dark web supplier and run ransomware on them which has been purchased from a different supplier. Many other services are offered in this ecosystem. Since it is global, hackers in one country can sell their services to cybercriminals in another.

3) Hacker-For-Hire Actors: The ENISA report described the Access-as-a-Service (AaaS) market. Commonly known as spyware, AaaS allows the user to access the contents of a victim's phone, potentially including the microphone and camera. The report predicted that this sector will be subject to increasing regulation on human rights as well as national security grounds. This prediction has been borne out by events. In November 2021, the U.S. blacklisted well-known AaaS firm NSO group [44], and Israel drastically reduced the number

of countries to which cyber-weapons could be exported [45]. The technology continued to cause controversy in 2022, with a stream of revelations including the discovery in February that Israel had used NSO spyware against some of its own public figures [46]. In April, use of NSO spyware for surveillance of Jordanian human rights defenders was revealed [47].

4) Hacktivists: Early hacktivism was generally associated with idealistic left-wing anti-corporate ideology. Hacktivists use cyberspace for activities related to political activism in the real world, aiming to increase awareness or to cause reputational damage to organisations. Hacktivism is typically not done for financial or material gain [48]. The ENISA report finds low current levels of hacktivism, but anticipates a possible rise in the future as environmental issues come to the fore. It notes that hacktivism can be faked by nation state actors to confuse attribution for subversive activities.

In October 2021, protests in Belarus over the disputed re-election of Alexander Lukashenko were accompanied by hacktivist activity, including the theft and release of information revealing the identities of Belarussian security agents [49].

B. Cybercrime threats in 2020-2021

1) Ransomware: Ransomware is the practice of encrypting the files on an organisation's devices and demanding a ransom for the decryption key. Since CryptoLocker first appeared in September 2013 [50], ransomware has become increasingly sophisticated. Recent escalation tactics include using Distributed Denial of Service (DDoS) [51], and threatening to expose sensitive data, including embarrassing data from the devices of organisational decision-makers [52]. Some hackers search networks for details of cybersecurity insurance coverage amounts, tailoring their ransom requests accordingly [50]. With an estimated $590 million of ransomware payments made in the first six months of 2021 [53], by November an insurance backlash had begun, with rises in premiums of up to 300% and steep falls in amounts covered [54].

Ransomware crews make their expertise available to franchisees in what is known as a Ransomware-as-a-Service model [55]. They take precautions to ensure that franchisees do not launch attacks in their home countries, often automating a check of the installed language on a system before file encryption [56]. Security journalist Brian Krebs suggested that installing certain Eastern European languages on a computer could provide protection against some ransomware strains [57].

The ENISA report describes how zero-day vulnerabilities, generally bought by nation-state actors, were in 2021 often used in sophisticated attacks on small numbers of very high-value ransomware targets, a practice known as big game hunting.

In June 2021, the U.S. government raised the priority of ransomware to the same level as terrorism [58]. Subsequent initiatives such as the international 'Counter Ransomware Initiative' [59] sought to improve international ransomware prevention and response. Priorities were increasing resilience, disrupting illicit finance and jurisdictional arbitrage, and improving international cooperation and diplomacy to encourage states to address ransomware operations within their own territories [60]. A series of arrests and forum shutdowns by Russian authorities in January and February 2022 was considered a change in Russian policy towards ransomware and other cybercrime [61]. Whether a conciliatory gesture towards the U.S. [62], or an attempt to keep China, also experiencing severe ransomware incursions [63], onside, enforcement diminished after Russia invaded Ukraine.

Industry commentators in early 2022 observed increased use of ransomware by nation state actors, such as a January fake ransomware attack on Ukrainian government sites, concluding that the ransomware cover provides deniability to an attacking state [64].

2) Cryptojacking: Often seen as a relatively victimless crime, cryptojacking is the practice of surreptitiously mining cryptocurrency on a user's device. When done at scale it can be lucrative [65]. ENISA reports that cryptojacking incidence was at its highest ever in the first quarter of 2021. It suggests that the rapid increase of cryptojacking and ransomware is facilitated by the ease with which they translate to financial gain, facilitated by the use of cryptocurrencies.

3) Other Cybercrime: While cryptojacking and ransomware require large-scale networks to function, there is also plenty of traditional crime on the Internet. In an analysis of the 'Digital Goods' or 'Services' dark web sales categories, Meland et al. [55] report that credit card fraud ('carding') is the most popular crime. Carding involves the bulk selling of credit card data, sometimes with card holders' personal details [66]. Stealing and selling credit card information at scale is easier online.

4) Cyberespionage: Cyberespionage is now an accepted part of geopolitics. Between December 2020 and February 2021, national infrastructure cyber-intrusions were reported by Finland (parliamentary email) [67], Japan (military contractor) [68], Malaysia (Armed Forces website) [69] and Ukraine (government document sharing) [70], to take just a few examples. In early 2021, intrusions on U.S. and other government networks via Sunburst (SolarWinds) and other supply chain attacks caused concern about the risk of cyberespionage. However, experts in the field expressed the view that this was merely traditional international jostling [43].

5) Cyber Patriotism: Not mentioned in the ENISA report, which concluded observations in mid-2021, there has been an outbreak of activity from what Recorded Future's Allan Liska calls 'cyber patriots' as a result of Russia's invasion of Ukraine. We distinguish cyber patriotism from hacktivism on the basis of its nationalist origins. Sharp divisions have occurred within cybercriminal groups that contained members from both Russia and Ukraine [71]. Many hacker groups have taken sides, vowing to leverage their skills to further their country's cause [72]. Others have also acted. After the notorious Conti ransomware group announced its support for Russia, a Ukrainian researcher, who had lurked on Conti servers for years, leaked thousands of documents containing their internal communications [73].

Cyber patriotism has had a direct impact on software security. Some software component projects on GitHub have been modified to become 'protestware,' displaying banners like 'Stand with Ukraine,' or facts about the invasion. In one case,

the popular 'vue-cli' framework had a component added that deleted all files on its host computer if it detected that it was running in Russia or Belarus. Brian Krebs reports concerns that such activities would '*erode public trust in open-source software*' [74]. Since blind trust in open source components is not conducive to software security, we argue that this might be a good thing.

6) Cyberwarfare: As it moves online, infrastructure is increasingly vulnerable to cyber outages. These can be caused by natural phenomena such as hurricanes. They can be collateral damage from criminal cyber activity, as the Colonial pipeline outage in the U.S. in May 2021 was. They can also be the result of actions by a hostile state. Cybersecurity organisation Recorded Future documented a large increase in suspected intrusion activity in India by Chinese state-sponsored groups during border tensions in 2020. Recorded Future stated that India's power sector and two seaports were targeted in a '*concerted campaign against India's critical infrastructure.*' Severe power outages in Mumbai on October 12 2020 were attributed to Chinese sabotage by Anil Deshmukh, a minister for Maharashtra state. China disputes the claim, but the fact that it was made at all reflects the uncertainty engendered by the mere possibility of cyberattack.

In 2010 the Stuxnet worm, widely attributed to Israel and the U.S., attacked industrial control systems in Iran. The Natanz uranium enrichment site was badly damaged, even though the Natanz network was supposedly air-gapped from the Internet. Stuxnet is considered to be the world's first cyber-weapon [75].

Prior to the February 2022 invasion of Ukraine, Russia-Ukraine history showed a gradual escalation from cyber-warfare to kinetic warfare. The electric grid in Ukraine was attacked on December 23rd 2015. In an incursion attributed by the DoJ to Russia's GRU [76], 30 substations were taken offline and power to 230,000 people in freezing temperatures was lost for up to 6 hours. There were related outages the following year. In 2017, an accounting tool used by approximately half of the businesses in Ukraine was infiltrated with fake ransomware in what became known as the NotPetya attack. There were huge financial costs to business. The Merck pharmaceutical company lost $1.4bn [77]. This incident was attributed to the Russian state by the UK government [78], but the apparently criminal method of attack allowed for plausible deniability. It was hugely destabilising in Ukraine, and served as a warning to international organisations considering doing business there, signalling that perhaps it would not be worth the trouble [79]. In 2020, the DoJ indicted six Russian nationals for the Ukrainian power cuts and the NotPetya attack, among other alleged crimes [76]. An unintended victim was the insurance industry, forced to contend with geopolitical questions around attribution and 'act of war' definitions in its attempts to avoid payouts [77].

In the build-up to the Russian invasion, cyberattacks on Ukraine increased, with data wipers disguised as ransomware [80], DDoS, bot farms spreading misinformation [81] and widespread infrastructure attacks [82]. A cyberattack on the day of the invasion on Viasat KA-SAT routers used in Ukrainian military communications had an impact on other European countries, with monitoring and control of wind turbines in Germany rendered unavailable [83]. Cyberattacks continued after the invasion [82]. Meanwhile, western officials warned amateur hackers against joining the voluntary 'IT Army of Ukraine,' organising on Telegram.

In a discussion on cybersecurity threat escalation on the website of the Arms Control Association (ACA), Michael T. Klare describes the inherent danger that a cyberattack on Nuclear Command, Control, and Communications (NC3) facilities would justify a nuclear response. The ACA views this as an unacceptable risk, suggesting that even the fear that NC3 facilities were under attack could trigger an escalation to the use of nuclear weapons. If tensions were high enough, even a simple power outage could cause a national leader to feel that their nuclear capability was in imminent danger. This could propel them into striking first [84]. The advent of cyber patriot vigilantes, some of them expert hackers, increases the risk of such an unanticipated outcome.

The danger that cyber incidents could cause escalation to kinetic warfare was raised by U.S. President Biden in 2021 [85]. It is likely to be considered by every nation when assessing the pros and cons of unfettered access to a global Internet.

IV. The Role of Software Vulnerabilities

We have discussed some of the forces pushing nations to separate from the global Internet, and outlined some threats likely to accelerate that process. We now turn to the role of software vulnerabilities in exacerbating those threats. A perusal of material from hacker training sites such as Bugcrowd University (https://www.bugcrowd.com/hackers/bugcrowd-university/) indicates that the discovery and use of software vulnerabilities is at the core of hacking techniques.

Vulnerabilities are mitigated by software patches. In a survey by *BAE Systems Applied Intelligence*, reported in May 2021 [86], 52% of recent security incidents were caused by missing patches. The mean time to patch was 205 days [87]. Patching strategies are complicated by the fact that software normally contains multiple open source software (OSS) components which may themselves include other libraries. One third of studied vulnerabilities in OSS were present for over three years before remediation [88]. December 2021 brought this issue to the fore with the publicising of the Log4j bug, in which a little-known feature of a ubiquitous Java logging component was discovered to be vulnerable to remote code execution [89].

Unfortunately, vulnerable systems are easily discoverable online. Actors wishing to exploit the latest defects can run tailored searches via sites such as Shodan [90], which will find and list Internet-facing systems with specified characteristics. Failure to patch is discoverable.

Not all software vulnerabilities are equal. In the U.S., NIST maintains the National Vulnerability Database, which collates reported software vulnerabilities and assigns a Common Vulnerability Scoring System (CVSS) score to them, with a 'Critical' 10.0 being the highest score available. High CVSS scores indicate that a vulnerability is simple to exploit, remotely available, and likely to result in a severe impact on the

vulnerable system. The term 'zero-day' is used to describe a critical software vulnerability that has not yet been patched, may not be generally known about, and possibly has not even been reported to the software manufacturer. Zero-days for popular software are much in demand and can be bought on the dark web [91]. National security agencies are known to stockpile zero-days for use in cyberespionage [92].

In April 2017, the 'Shadow Brokers' published a number of hacking tools widely reputed to originate with the U.S. National Security Agency (NSA) [93]. These leveraged serious bugs such as the Eternal Blue exploit (CVE-2017-0144), which the NSA had reputedly used for several years [92]. Microsoft had been notified of the theft of the exploit, and released a patch for Eternal Blue a month before it was published [94]. Nevertheless, sufficient machines remained unpatched for the WannaCry ransomware cryptoworm attack of May 12 2017 and the NotPetya attack of June 27 2017 to cause worldwide havoc. The Eternal Blue SMB exploit allowed WannaCry and NotPetya to spread and self-propagate without any user intervention [95], [96]. Until it was patched, Eternal Blue was present on all versions of Windows from at least Windows 2000.

Another long-lived critical Microsoft defect was the 'Zerologon' elevation-of-privilege bug. Quietly patched in August 2020 and made public the following month, it infected Windows Server 2008 and all newer versions of Windows Server up to 2019 [97]. The persistence of Eternal Blue and Zerologon for over a decade after Microsoft mandated internal use of Microsoft Security Development Lifecycle (MS-SDL) is a reminder that there are no software security silver bullets.

The relatively collegiate international atmosphere that had surrounded defect discovery and notification began to change in 2018, when the Chinese government banned Chinese security researchers from participating in vulnerability discovery competitions such as CanSecWest's Pwn2Own [98], in which they had previously been highly successful. In 2021, the Cyberspace Administration of China introduced rules forbidding the sale of vulnerabilities or the notification of vulnerabilities to overseas entities other than the manufacturers. Organisations discovering vulnerabilities in their own code must notify them to the Chinese government within two days [99]. For entities trading within China, this could put them in a position of having to notify the Chinese government about vulnerabilities before a patch is in place. Organisations are 'encouraged,' though not obliged, to notify the government first about vulnerabilities discovered in other organisations' code. In December 2021, AliBaba Cloud was suspended from an information-sharing partnership with China's Ministry of Industry and Information Technology (MIIT) for failure to notify it about the Log4j vulnerability. AliBaba staff notified Apache on November 24, while the MIIT was not notified until December 9 [100].

Considered in light of the move by some countries to use only homegrown software internally, these developments could presage a time when foreign adversaries are familiar with the software used by the U.S. and the EU, and its vulnerabilities,, while the reverse is no longer true.

V. Attempts to Remediate

Having seen the impact of software vulnerabilities on software quality, we now look at approaches in industry and academia to reducing software vulnerabilities. We consider some of the shortcomings of existing approaches and suggest some reasons why they are not effective. We also discuss recent legislation relating to software security in Europe and the U.S.

A. Industry

Focus on software security in industry varies depending on the industry involved. In the U.S., NIST publishes comprehensive cybersecurity guidelines. Revision 5 of NIST Special Publication 800-53, 'Security and Privacy Controls for Information Systems and Organizations' was published in September 2020 [101]. The guide is used by safety-critical industries; for example, U.S. Nuclear Regulatory Commission Regulatory Guide 5.71, on cybersecurity programmes for nuclear facilities, used NIST 800-53 version 3 to provide a comprehensive cybersecurity approach [102]. Weighing in at a hefty 465 pages, version 5 provides descriptions of numerous cybersecurity controls but includes a mere four pages on 'Developer Testing and Evaluation.' This software development section outlines nine activities that would be familiar to most software security advocates.

Software security methodologies in general use in industry include MS-SDL, Software Assurance Maturity Model, Building Security In Maturity Model, Common Criteria and various ISO standards. All coalesce around a number of activities which are regularly synthesised in academic papers [103] [104], such as threat modelling, use of analysis tools and penetration testing. However, the software development security industry is currently convulsed by software developers' move away from regular, relatively infrequent releases, to which blocking 'security gates' can be applied, to automated continuous releases. This move is facilitated by the DevOps emphasis on comprehensive automated tests. DevSecOps attempts to bring security into the DevOps approach, adding security tests to the automated test suite and automating security gates. Advocates of DevSecOps suggest that it 'shifts security to the left,' making it an issue that architects and developers must consider instead of something that is assessed just before release. Done well, DevSecOps can add predictability and credibility to a development team's security stance. However, practitioners express concerns about whether comprehensive security checks can ever be fully automated [105]. Done badly, DevSecOps adds little value and can even have a negative impact on a development process [106].

B. Academia

Much work has been done in academia on how software can be made more secure. Wurster and von Oorschot [107] argued that software developers, though seen as warriors in the forefront of the battle for secure software, are in fact part of the problem since they have multiple, often conflicting, priorities and are rarely security experts. They suggested that developer tools should be created with usability in mind, and

should make it difficult for developers to code insecurely. They pointed out that developer security training was often still advocated as the solution for developers. They identified an issue with developers who are either unaware of, or who ignore, new security technologies, and noted that security technologies which must be independently run by developers (i.e. they are not embedded in standard tools) will not be run by all developers. They advocated 'security mechanisms which are invisible to the application developer.' This theme was developed by Xie et al. [108], who looked at why programmers make security errors, concluding that developers often feel that someone else is responsible for security and it is not their concern. Acar et al. [109] discussed how 20 years of lessons learned from usable security work can be applied in security research with software developers, and derived a research agenda on these lines. Green and Smith [110] discussed simplifying security APIs to make them less impenetrable to programmers, proposing ten principles for creating secure and usable crypto APIs.

A recurring research theme is that developers, who have other priorities, lack the training and expertise necessary for security proficiency. Weir et al. [111], the Motivating Jenny team (https://motivatingjenny.org/) and others have looked at interventions and tools to help teams to code securely. However, in a 2020 review of top U.S. Computer Science (CS) undergraduate courses, Almansoori et al. [112] found that security-unaware use of insecure C++ functions was passed from teachers to students. Moreover, in all cases there was no mandatory formal secure coding component to the CS course. We argue that while *ad hoc* on-the-job training efforts have value, software security is so critical that it should be automatically embedded in all software development training.

The academic record includes valuable accounts of actual industry practice. Sadowski et al. [113] described the development of a static analysis tool at Google, a model for what can be done in a cohesive environment, even a very large one. By contrast, Morales et al.'s [106] account of a dysfunctional multi-year development by a main contractor using multiple subcontractors with a DevSecOps pipeline gives excellent insight into the ease with which organisational dynamics can damage security outcomes. Previous work [114] highlighted that management security buy-in is vital. Swift software security progress is tied to upper management concern, which may be enhanced by increased regulatory and legal incentives.

C. Legislation

Both Europe and the U.S. appear to be moving towards regulations for secure software, a welcome recognition of the increasing importance of the field. Here, we give a brief overview of relevant developments.

GDPR: The EU's General Data Protection Regulation (GDPR), which governs the protection of personal data in the European Economic Area, came into force in 2018. It mandates obtaining subjects' permission for data storage, sets time limits on data retention, and allows for penalties where data is inappropriately shared. Although the GDPR was not created with the primary aim of enhancing software security it has had this effect, since a data breach could expose the organisation to financial penalties. It does not list explicit cybersecurity requirements, instead using broad phrases such as 'state of the art.' This deters a 'checkbox' security mentality, encouraging awareness of ongoing software security developments [115].

The NIS Directive and ENISA: The EU's 2016 NIS Directive dealt with cybersecurity but did not discuss secure software development [116], though this should change with NIS2. A thoughtful and well-researched preparatory paper from ENISA outlines the current EU work on introducing security certification for software, with consideration of existing standards and certifications, and likely pitfalls [117]. This welcome move towards EU-level certification should be expedited.

The UK: The UK's 'Government Cyber Security Strategy 2022-2030,' released in February 2022, lists aspirations around a 'secure by design' framework to be adopted by the UK [118]. No specific advice for software development is available yet.

The U.S.: In a week in May 2021 in which the ransomware shutdown of an essential U.S. oil pipeline dominated the news, the U.S. President released an 'Executive order on Improving the Nation's Cybersecurity,' which provides specific software-related measures. Part a) asserts that *'the Federal Government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software.'* NIST is required to identify guidelines to evaluate software security and the security practices of developers and suppliers, and to identify *'tools or methods to demonstrate conformance with secure practices.'* Enhancing supply chain security, securing build environments, automating supply chain assurance and providing evidence for these activities are discussed. Identifying 'critical' software is also addressed, as is Internet of Things (IoT) security and a suggested security labelling system for software and IoT devices. U.S. government agencies will be obliged to consider software security when engaging in or renewing critical software contracts. Legacy code that cannot comply with the new requirements will have to be replaced. Steps to secure the software supply chain will be kept under review, with a progress report required within a year of the signing of the order.

D. Exacerbating Factors

There is an essential imbalance in the software security world. Most software developers prioritise functionality [119], followed by efficiency [105], elegant design, or maintainability. Unless they are working for an organisation that emphasises security, they will probably not put security first. In fact, even if they work for a security organisation, their security practice could be suspect [120].

While software developers struggle with time-to-market and tight deadlines, hackers, security researchers and red-teamers can focus solely on finding the security defects inadvertently left by developers, and exploiting them. When it comes to training, they have multiple resources at their disposal such as the free Bugcrowd University and the many dozens of courses annually at Black Hat and elsewhere geared towards 'penetration testers.'

This imbalance of time and resources is difficult to tackle. Many software developers have not received training in secure coding. Organisations often have relatively few, if any, software security staff; a single software security expert supporting one or two hundred developers is not uncommon [121]. Outside of regulated industries, there is currently little incentive for organisations to prioritise security over time-to-market, and some organisations have no security process at all [103].

E. A 'Zero Tolerance' Approach to Software Security

We argue that the software industry now needs to step up and adopt a 'zero tolerance' approach to software security issues. Haney et al. [122] described how organisations that successfully deliver secure software have a 'security culture.' The entire software industry needs to develop a 'security culture,' with a comprehensive upgrade of education, tools, and documentation.

The building blocks to achieving this are not novel. They involve steps that are both widely acknowledged as necessary, and widely ignored. Cultural change is needed in education, from universities to boot camps. It should be unacceptable to teach computer skills without including mandatory security awareness and associated training.

At the corporate level, too often security risk assessments end with a decision to increase insurance provision against cyberattack. The balance of risk must be changed. This can be done by making organisations liable for costs incurred due to secure coding negligence on their part. Some experts argue that mandating secure coding would impose the type of procedural rigidity that leads to an obsession with passing tests, as can happen in the payments industry [123]. However, the flexible wording of the GDPR gives an insight into how secure coding can be mandated without leading to a checkbox mentality. In any case, even a checkbox mentality would be a vast improvement on the current security posture of many organisations [124].

VI. Conclusion

As we have seen, crime and other aggressive behaviour on the Internet thrives on the existence of software vulnerabilities. A steady supply of zero-days, combined with delays in patching known vulnerabilities, ensures that bad actors can continue to exploit weaknesses for financial or other gain. This state of affairs causes an unsustainable level of uncertainty and risk. The threat of industrial sabotage or breach of military command and control structures from foreign actors adds to the mounting pressures on the global Internet, pushing it towards further fragmentation.

We have also seen how the opportunities for incursion provided by a global Internet can have a destabilising effect on existing power balances. If software security is not taken sufficiently seriously, there is a danger that national administrations will increasingly judge that the price of participating in a global network is too high. National executives may even decide that retreating to a national or regional Intranet would enhance their national security and reduce the danger of cyberattack on NC3 facilities and other critical infrastructure. As incidents of damage from cyber activities increase globally, assessments of this type may not be confined to authoritarian regimes. Though some states might welcome a fragmentation of the Internet, it seems like a failure of human imagination and potential.

The complete elimination of software vulnerabilities may be impossible, but a drastic reduction is not. It is time for a less accommodating approach. A 'zero tolerance' attitude to software security issues should be adopted, and it should include cultural and legislative change. This would reduce the perceived vulnerability of vital systems and help to maintain confidence in a networked world.

Acknowledgment

SFI grants 18/CRT/6222, 13/RC/2077_P2, 13/RC/2094_P2.

References

[1] S. Hoffmann, D. Lazanski, and E. Taylor, "Standardising the Splinternet: how China's technical standards could fragment the Internet," *J. Cyber Policy*, vol. 5, 2020.

[2] S. Harrison, "Cyber attack: When will the Irish health service get a resolution?" https://www.bbc.com/news/world-europe-57193160, 2020.

[3] R. Lakshmanan, "Exclusive: SonicWall hacked using 0-day bugs in its own VPN product," https://thehackernews.com/2021/01/exclusive-sonicwall-hacked-using-0-day.html, 2021.

[4] B. Dickson, "AV Oracle: New hacking technique leverages antivirus to steal secrets," https://portswigger.net/daily-swig/av-oracle-new-hacking-technique-leverages-antivirus-to-steal-secrets, 2019.

[5] M. Korolov, "Cisco router vulnerability puts network segmentation at risk," https://www.datacenterknowledge.com/security/cisco-router-vulnerability-puts-network-segmentation-risk, 2020.

[6] A. O'Driscoll, "25+ cyber security vulnerability statistics and facts of 2021," https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/, 2021.

[7] E. Claessen, "Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU," *J. Cyber Policy*, vol. 5, no. 1, 2020.

[8] D. Dominey-Howes, "The Tonga volcanic eruption reveals the vulnerabilities in our global telecommunication system," https://techxplore.com/news/2022-01-tonga-volcanic-eruption-reveals-vulnerabilities.html.

[9] E. Buchanan, "Subsea cables in a thawing Arctic," https://www.maritime-executive.com/editorials/subsea-cables-in-a-thawing-arctic, 2018.

[10] C. Gallagher, "Russian military drills pose strategic and environmental risks to Ireland," https://www.irishtimes.com/news/ireland/irish-news/russian-military-drills-pose-strategic-and-environmental-risks-to-ireland-1.4784787.

[11] K. Ermoshina, B. Loveluck, and F. Musiani, "A market of black boxes: The political economy of Internet surveillance and censorship in Russia," *Journal of Information Technology & Politics*, 2021.

[12] FCC, "Circuit capacity data for U.S.-international submarine cables," https://www.fcc.gov/international/circuit-capacity-data-us-international-submarine-cables, 2022.

[13] J. Smith, "Internet Atlas maps the physical internet to enhance security," https://news.wisc.edu/internet-atlas-maps-the-physical-internet-to-enhance-security/, 2021.

[14] D. Temple-Raston, "Report: Beijing, Moscow step up efforts to control the Internet's backbone," https://therecord.media/report-beijing-moscow-step-up-efforts-to-control-the-internets-backbone/, 2021.

[15] H. Fouquet, "China's 7,500-mile undersea cable to Europe fuels Internet feud," https://www.msn.com/en-us/money/other/china-e2-80-99s-7500-mile-undersea-cable-to-europe-fuels-internet-feud/ar-BB1egCN9.

[16] J. Sherman, "The US-China battle over the Internet goes under the sea," https://www.wired.com/story/opinion-the-us-china-battle-over-the-internet-goes-under-the-sea/, 2020.

[17] M. Cartwright, "Internationalising state power through the Internet: Google, Huawei and geopolitical struggle," *Internet Policy Review*, vol. 9, no. 3, 2020.

[18] J. Dunleavy, "FCC designates Huawei and four other Chinese tech companies as national security threats," https://www.washingtonexaminer.com/news/fcc-huawei-four-other-chinese-tech-companies-national-security-threats, 2021.

[19] Cloudflare, "What is an Internet exchange point? — How do IXPs work?" https://www.cloudflare.com/learning/cdn/glossary/internet-exchange-point-ixp/, 2019.

[20] D. McCullagh, "How Pakistan knocked YouTube offline (and how to make sure it never happens again)," https://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/, 2008.

[21] V. Ververis, S. Marguel, and B. Fabian, "Cross-country comparison of Internet censorship: A literature review," *Policy Internet*, vol. 12, no. 4, 2020.

[22] K. Limonier, F. Douzet, L. Pétiniaud, L. Salamatian, and K. Salamatian, "Mapping the routes of the Internet for geopolitics: The case of Eastern Ukraine," *First Monday*, 2021.

[23] W. J. Drake, V. G. Cerf, and W. Kleinwächter, "Internet fragmentation: An overview," *World Economic Forum*, p. 80, 2016.

[24] Z. Chen, C. Wang, G. Li, Z. Lou, S. Jiang, and A. Galis, "NEW IP framework and protocol for future applications," in *NOMS 2020*, 2020.

[25] R. D. Taylor, ""Data localization": The Internet in the balance," *Telecommunications Policy*, vol. 44, no. 8, 2020.

[26] J. Silva, "LinkedIn is shutting down in China, will be replaced by a new app called InJobs," https://www.techspot.com/news/91754-linkedin-shutting-down-china-replaced-new-app-called.html, 2021.

[27] R. Harb, "India bans a further 118 Chinese apps as physical and online tensions escalate," https://www.theregister.com/2020/09/03/india_bans_chinese_apps/.

[28] D. Goodin, "FCC puts Kaspersky on security threat list, says it poses "unacceptable risk"," https://arstechnica.com/information-technology/2022/03/fcc-puts-kaspersky-on-security-threat-list-says-it-poses-unacceptable-risk/.

[29] F. House, "Countries - Internet freedom scores," https://freedomhouse.org/countries/freedom-net/scores, 2021.

[30] A. A. Niaki, S. Cho, Z. Weinberg, N. P. Hoang, A. Razaghpanah, N. Christin, and P. Gill, "ICLab: A global, longitudinal Internet censorship measurement platform," in *IEEE SP 2020*, 2020.

[31] B. Duggan, "Uganda shuts down social media; candidates arrested on election day," https://edition.cnn.com/2016/02/18/world/uganda-election-social-media-shutdown/index.html.

[32] HRW, "Belarus: Internet disruptions, online censorship," https://www.hrw.org/news/2020/08/28/belarus-internet-disruptions-online-censorship, 2020.

[33] BBC, "Kazakhstan unrest: Internet cut amid fuel protests," https://www.bbc.com/news/world-asia-59876093, 2022.

[34] C. Cimpanu, "Oracle: China's internet is designed more like an intranet," https://www.zdnet.com/article/oracle-chinas-internet-is-designed-more-like-an-intranet/, 2019.

[35] ——, "Two of China's largest tech firms are uniting to create a new 'domestic OS'," https://www.zdnet.com/article/two-of-chinas-largest-tech-firms-are-uniting-to-create-a-new-domestic-os/, 2019.

[36] "Russia to launch 'independent internet' for BRICS nations - report," https://www.rt.com/russia/411156-russia-to-launch-independent-internet/.

[37] BBC, "Russia bans sale of gadgets without Russian-made software," https://www.bbc.com/news/world-europe-50507849, 2019.

[38] S. Jarman, "How pulling out of Russia's internet could further isolate its citizens," https://bigthink.com/the-present/russian-internet-runet/?utm_medium=Social&utm_source=Twitter#Echobox=1648510641-2.

[39] H. F. Ukraine, "Companies suspending operations in Russia and Belarus," https://hrforukraine.notion.site/Companies-Suspending-Operations-in-Russia-and-Belarus-93d42cbb7a234438b663bded9f1f7f4c.

[40] S. Fadilpašić, "ICANN rejects call to remove Russian domains from the Internet," https://www.msn.com/en-us/news/technology/icann-rejects-call-to-remove-russian-domains-from-the-internet/ar-AAUBABO.

[41] J. Parsons, "Russians 'to be disconnected from global internet from Friday'," https://metro.co.uk/2022/03/07/russia-preparing-to-disconnect-from-global-internet-on-march-11-16230918/.

[42] EU, *ENISA threat landscape 2021: April 2020 to mid July 2021*. Publications Office, 2021.

[43] T. Wheeler, "The danger in calling the SolarWinds breach an 'act of war'," https://www.brookings.edu/techstream/the-danger-in-calling-the-solarwinds-breach-an-act-of-war/, 2021.

[44] BBC, "NSO Group: Israeli spyware company added to US trade blacklist," https://www.bbc.com/news/technology-59149651, 2021.

[45] C. Cimpanu, "Israel restricts cyberweapons export list by two-thirds, from 102 to 37 countries," https://therecord.media/israel-restricts-cyberweapons-export-list-by-two-thirds-from-102-to-37-countries/.

[46] Reuters, "Israel ramps up scrutiny of police as NSO scandal spreads," https://www.euronews.com/2022/02/07/us-israel-nso.

[47] FLD, "Report: Jordanian human rights defenders and journalists hacked with Pegasus spyware," https://www.frontlinedefenders.org/en/statement-report/report-jordanian-human-rights-defenders-and-journalists-hacked-pegasus-spyware.

[48] A. Pawlicka, M. Choraś, and M. Pawlicki, "Cyberspace threats," in *ARES '20*, 2020.

[49] O. Carroll, "Hacktivists vs The Dictator: How Belarus cyber army is taking on Alexander Lukashenko and his goons," https://www.independent.co.uk/news/world/europe/belarus-lukashenko-protests-cyber-attacks-minsk-b807184.html, 2021.

[50] S. Greengard, "The worsening state of ransomware," *Commun. ACM*, vol. 64, no. 4, Apr 2021.

[51] D. S. Amanda Tanner, Alex Hinchliffe, "Threat assessment: Blackcat ransomware," https://unit42.paloaltonetworks.com/blackcat-ransomware/.

[52] C. Cimpanu, "Some ransomware gangs are going after top execs to pressure companies into paying," https://www.zdnet.com/article/some-ransomware-gangs-are-going-after-top-execs-to-pressure-companies-into-paying/, 2021.

[53] "Treasury continues to counter ransomware as part of whole-of-government effort; sanctions ransomware operators and virtual currency exchange," https://home.treasury.gov/news/press-releases/jy0471.

[54] C. Cohn, "Insurers run from ransomware cover as losses mount," https://www.reuters.com/markets/europe/insurers-run-ransomware-cover-losses-mount-2021-11-19/, 2021.

[55] P. H. Meland, Y. F. F. Bayoumy, and G. Sindre, "The Ransomware-as-a-Service economy within the darknet," *Computers & Security*, vol. 92, 2020.

[56] C. Nocturnus, "Cybereason vs. DarkSide Ransomware," https://www.cybereason.com/blog/cybereason-vs-darkside-ransomware.

[57] B. Krebs, "Try this one weird trick Russian hackers hate," https://krebsonsecurity.com/2021/05/try-this-one-weird-trick-russian-hackers-hate, 2021.

[58] M. Sharma, "US will give ransomware hacks similar priority to terrorist attacks," https://www.techradar.com/uk/news/us-will-give-ransomware-hacks-similar-priority-to-terrorist-attacks.

[59] A. Neuberger, "Update on the International Counter-Ransomware Initiative," https://www.state.gov/briefings-foreign-press-centers/update-on-the-international-counter-ransomware-initiative.

[60] T. SpiderLabs, "Law enforcement collaboration has Eastern-European cybercriminals questioning whether there is a safe haven anymore," https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/law-enforcement-collaboration-has-eastern-european-cybercriminals-questioning-whether-there-is-a-safe-haven-anymore/, 2021.

[61] A. Vicens, "Russian government continues crackdown on cybercriminals," https://www.cyberscoop.com/sky-fraud-takedown-russia-cybercrime/.

[62] M. I. Nicole Sganga, "Russia arrests 14 alleged members of REvil ransomware gang," https://www.cbsnews.com/news/ransomware-russia-arrests-revil/, 2022.

[63] T. Uren, "Srsly risky biz: Thursday January 13," https://srslyriskybiz.substack.com/p/srsly-risky-biz-thursday-january-39c.

[64] C. Team, "As ransomware payments continue to grow, so too does ransomware's role in geopolitical conflict," https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/.

[65] S. Pastrana and G. Suarez-Tangil, "A first look at the crypto-mining malware ecosystem: A decade of unrestricted wealth," in *IMC*, 2019.

[66] P.-Y. Du, N. Zhang, M. Ebrahimi, S. Samtani, B. Lazarine, N. Arnold, R. Dunn, S. Suntwal, G. Angeles, R. Schweitzer, and et al., "Identifying, collecting, and presenting hacker community data: Forums, IRC, carding shops, and DNMs," in *ISI 2018*, 2018.

[67] C. Cimpanu, "Finland says hackers accessed MPs' emails accounts," https://www.zdnet.com/article/finland-says-hackers-accessed-mps-emails-accounts/, 2020.

[68] "Kawasaki Heavy hack may have targeted defense-linked information," https://proteuscyber.com/privacy-database/news/3014-kawasaki-heavy-hack-may-have-targeted-defense-linked-information-the-japan-times.

[69] "Malaysia's armed forces confirms cyber-attack on network," https://www.straitstimes.com/asia/se-asia/malaysias-armed-forces-confirms-cyber-attack-on-network, 2020.

[70] "The NCCC at the NSDC of Ukraine warns of a cyberattack on the document management system of state bodies," https://www.rnbo.gov.ua/en/Diialnist/4823.html, 2021.

[71] J. Uchill, "After Conti backs war, ransomware gangs realize peril of patriotism amid infighting," https://www.scmagazine.com/analysis/ransomware/after-conti-backs-war-ransomware-gangs-realize-peril-of-patriotism-amid-infighting.

[72] E. Vail, "Russia or Ukraine: Hacking groups take sides," https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/.

[73] S. Lyngaas, "'I can fight with a keyboard': How one Ukrainian IT specialist exposed a notorious Russian ransomware gang," https://edition.cnn.com/2022/03/30/politics/ukraine-hack-russian-ransomware-gang/index.html.

[74] B. Krebs, "Pro-Ukraine 'protestware' pushes antiwar ads, geo-targeted malware," https://krebsonsecurity.com/2022/03/pro-ukraine-protestware-pushes-antiwar-ads-geo-targeted-malware/.

[75] B. Bakić, M. Milić, I. Antović, D. Savić, and T. Stojanović, "10 years since Stuxnet: What have we learned from this mysterious computer software worm?" in *IT 2021*, 2021.

[76] DoJ, "Six Russian GRU officers charged in connection with worldwide deployment of destructive malware and other disruptive actions in cyberspace," https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[77] J. Wolff, "Should insurance companies pay out for damage caused by state-sponsored cyberattacks?" https://slate.com/technology/2022/01/merck-notpetya-cyberattack-insurance-russia.html.

[78] "Foreign Office Minister condemns Russia for NotPetya attacks," https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks, 2018.

[79] Security Encyclopedia, "NotPetya," https://www.hypr.com/notpetya/.

[80] C. Cimpanu, "Microsoft: Data-wiping malware disguised as ransomware targets Ukraine again," https://therecord.media/microsoft-data-wiping-malware-disguised-as-ransomware-targets-ukraine-again/.

[81] ——, "Ukraine dismantles social media bot farm spreading "panic"," https://therecord.media/ukraine-dismantles-social-media-bot-farm-spreading-panic/.

[82] "Cyber attacks on Ukraine: DDoS, new data wiper, cloned websites, and Cyclops Blink," https://behaviour-group.com/PT/cyber-attacks-on-ukraine-ddos-new-data-wiper-cloned-websites-and-cyclops-blink.

[83] J. A. Guerrero-Saade, "AcidRain — A Modem Wiper Rains Down on Europe," https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/.

[84] M. T. Klare, "Cyber battles, nuclear outcomes? Dangerous new pathways to escalation," https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation.

[85] N. Bose, "Biden: If U.S. has 'real shooting war' it could be result of cyber attacks," https://www.reuters.com/world/biden-warns-cyber-attacks-could-lead-a-real-shooting-war-2021-07-27/.

[86] P. Muncaster, "Half of government security incidents caused by missing patches," https://www.infosecurity-magazine.com/news/half-government-incidents-missing/.

[87] J. Greig, "Average time to fix critical cybersecurity vulnerabilities is 205 days: report," https://www.zdnet.com/article/average-time-to-fix-critical-cybersecurity-vulnerabilities-is-205-days-report/, 2019.

[88] F. Li and V. Paxson, "A large-scale empirical study of security patches," in *CCS 2017*, 2017.

[89] CISA, "Apache Log4j vulnerability guidance," https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance.

[90] M. Bada and I. Pete, "An exploration of the cybercrime ecosystem around Shodan," in *IOTSMS 2020*, 2020.

[91] S. Rosenblatt, "How the shady zero-day sales game is evolving," https://www.darkreading.com/edge-articles/how-the-shady-zero-day-sales-game-is-evolving, 2021.

[92] S. B. Wicker, "The ethics of zero-day exploits—: the NSA meets the trolley car," *Commun. ACM*, vol. 64, no. 1, 2020.

[93] L. H. Newman, "The leaked NSA spy tool that hacked the world," https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/, 2018.

[94] SentinelOne, "Eternalblue exploit: What it is and how it works," https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/, 2019.

[95] A. McNeil, "How did the WannaCry ransomworm spread?" https://blog.malwarebytes.com/cybercrime/2017/05/how-did-wannacry-ransomworm-spread/, 2019.

[96] D. Bisson, "NotPetya: Timeline of a ransomworm," https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/.

[97] T. Tervoort, "Zerologon:Unauthenticated domain controller compromise by subverting Netlogon cryptography (CVE-2020-1472)," https://www.secura.com/uploads/whitepapers/Zerologon.pdf, 2020.

[98] C. Bing, "China's government is keeping its security researchers from attending conferences," https://www.cyberscoop.com/pwn2own-chinese-researchers-360-technologies-trend-micro/, 2018.

[99] "Chinese government lays out new vulnerability disclosure rules," https://therecord.media/chinese-government-lays-out-new-vulnerability-disclosure-rules/.

[100] X. Shen, "Apache Log4j bug: China's industry ministry pulls support from Alibaba Cloud for not reporting flaw to government first," https://www.scmp.com/tech/big-tech/article/3160670/apache-log4j-bug-chinas-industry-ministry-pulls-support-alibaba-cloud, 2021.

[101] NIST, *Security and Privacy Controls for Information Systems and Organizations*. National Institute of Standards and Technology, Sep 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[102] "Cyber security programs for nuclear facilities," https://scp.nrc.gov/slo/regguide571.pdf, 2010.

[103] H. Assal and S. Chiasson, "Security in the software development lifecycle," in *SOUPS*, 2018.

[104] P. Morrison, "A security practices evaluation framework," in *ICSE*, 2015.

[105] N. Tomas, J. Li, and H. Huang, "An empirical study on culture, automation, measurement, and sharing of DevSecOps," in *Cyber Security*, 2019.

[106] J. A. Morales, T. P. Scanlon, A. Volkmann, J. Yankel, and H. Yasar, "Security impacts of sub-optimal DevSecOps implementations in a highly regulated environment," in *ARES '20*, 2020.

[107] G. Wurster and P. van Oorschot, "The developer is the enemy," in *NSPW*, 2008.

[108] J. Xie, H. R. Lipford, and B. Chu, "Why do programmers make security errors?" in *VL/HCC 2011*, 2011.

[109] Y. Acar, S. Fahl, and M. L. Mazurek, "You are not your developer, either: A research agenda for usable security and privacy research beyond end users," in *SecDev 2016*, 2016.

[110] M. Green and M. Smith, "Developers are not the enemy!: The need for usable security APIs," *IEEE S&P 2016*, vol. 14, no. 5, 2016.

[111] C. Weir, I. Becker, J. Noble, L. Blair, M. A. Sasse, and A. Rashid, "Interventions for long-term software security: Creating a lightweight program of assurance techniques for developers," *SPE*, vol. 50, 2020.

[112] M. Almansoori, J. Lam, E. Fang, K. Mulligan, A. G. Soosai Raj, and R. Chatterjee, "How secure are our computer systems courses?" in *ICER 20*, 2020.

[113] C. Sadowski, E. Aftandilian, A. Eagle, L. Miller-Cushon, and C. Jaspan, "Lessons from building static analysis tools at Google," *Commun. ACM*, vol. 61, no. 4, 2018.

[114] I. Ryan, U. Roedig, and K.-J. Stol, "Understanding developer security archetypes," in *ICSE EnCyCriS*. ACM, 2021.

[115] G. P. De Francesco, "The general data protection regulation's practical impact on software architecture," *Computer*, vol. 52, no. 4, 2019.

[116] EU, "Directive (EU) 2016/1148 of the European Parliament and of the Council," https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[117] R. van der Veer, M. Valkema, F. Guasconi, and P. Drogkaris, *Advancing software security in the EU: the role of the EU cybersecurity certification framework*. ENISA, 2020.

[118] HM Government, "Government Cyber Security Strategy," 2022.

[119] A. Naiakshina, A. Danilova, E. Gerlitz, E. von Zezschwitz, and M. Smith, ""If you want, I can store the encrypted password": A password-storage field study with freelance developers," in *CHI 2019*, 2019.

[120] A. Greenberg, "The full story of the stunning RSA hack can finally be told," https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/.

[121] T. W. Thomas, M. Tabassum, B. Chu, and H. Lipford, "Security during application development: An application security expert perspective," in *CHI 2018*, 2018.

[122] J. Haney, M. Theofanos, Y. Acar, and S. Spickard Prettyman, ""we make it a big deal in the company": Security mindsets in organizations that develop cryptographic products," in *SOUPS 2018*, 2018.

[123] S. Rahaman, G. Wang, and D. D. Yao, "Security certification in payment card industry: Testbeds , measurements , and recommendations," *ACM CCS*, p. 481–498, 2019.

[124] L. Vaas, "BillQuick Billing App Rigged to Inflict Ransomware," https://vulners.com/threatpost/THREATPOST:94E54481AD472743701D499DC7677008.