Bug Bounties: Between New Regulations and Geopolitical Dynamics

Jantje Silomon, Mischa Hansel and Fabiola Schwarz
Institute for Peace Research and Security Policy, Hamburg, Germany
silomon@ifsh.de
hansel@ifsh.de
schwarz@ifsh.de

Abstract: Crowdsourced security and vulnerability co-ordination platforms, such as Bugcrowd or HackerOne, reward individuals for discovering, reporting, and responsibly disclosing software bugs. A growing number of vendors are turning towards these platforms to improve their product's security, whilst others set up their own bug bounty programs (BBPs) alongside more traditional approaches, such as in-house testing and professional security reviews. Whether providing a supplementary or even alternative path to organisational cybersecurity, these newer approaches go beyond increasing product security, for example by fostering co-operation between various actors or providing a clear incentive to remain on the ethical side of security research. Whilst some research centres on the reward structures, actor motivations, or effectiveness, the wider impact on peace and stability in cyberspace is rarely examined. Similarly, rarely is light shed on emerging regulatory or policy approaches, or the effects this might have. To fill these gaps, the paper will use Global Public Goods (GPGs) theory to example BBPs across two case studies. Whereas the novel Chinese regulations push towards more national sovereignty in cyberspace, the European Union invests in the compensation of BBP under-provision among open source software (OSS). These regulatory changes in China and endeavours by the European Union, respectively, reveal that the prevalent geopolitical divisions in related topics, such as internet governance, continue to play their part. Further research on BBPs is proposed to quantitatively examine their effect on peace and stability.

Keywords: Bug Bounty Programs, Vulnerability Disclosures, Global Public Goods, Geopolitical Dynamics

1. Introduction

As weak points are an inherent part of computer systems, various forms of vulnerability management have emerged over the years, ranging from best practices to responsible disclosure programs. Processes have become more formalised and security researchers are no longer left in the dark, having "to identify potential buyers, to determine accurate prices, and to overcome various barriers in executing a sale" (Kuehn, 2018). One example are BBPs, either hosted on platforms or created by vendors themselves, open to the public or by invitation only. These reward individuals for discovering and reporting software bugs, with the pay-out usually depending on the severity of the vulnerability (Malladi and Subramanian, 2019). There are also other intermediaries, some of which have come under scrutiny for also selling to disreputable entities (Perlroth, 2021; Coble, 2020).

Most BBPs set out specific criteria, including scope, submission and review processes, time constraints, as well as terms and conditions. These programs might focus on a single product, an element thereof, encompass an entire product suite or vulnerability type. Vulnerability information usually becomes public in line with responsible disclosure processes by the companies and platforms. Until recently, BBPs have remained rather apolitical. However, with growing success and publicity, there is also a rise in political alertness. Public institutions, such as the US Pentagon (Chatfield and Reddick, 2017) or the EU, have started to offer BBPs to secure their own networks or enhance OSS security, respectively. Questions regarding responsibility have arisen, from debates on product lifecycle support and its extension to whether or not vulnerability information is a public good. The latter in particular is of interest here in light of new regulations having come into effect in China as of September 2021 (CAC, 2021).

Against this backdrop, the paper will first delve into GPG theory before arguing why aspects of BBPs should be treated as such. Next, two empirical case studies with different focal points will be analysed, beginning with China and followed by the European Union. The former centres on new regulatory changes and extrapolates how these might affect BBPs, and cyber security more broadly. The latter addresses a specific programme that attempts to deal with OSS security. A preliminary model is then formed and discussed prior to concluding remarks.

2. Global Public Goods Theory

A public good combines two qualities, namely non-rivalry and non-excludability. Non-rivalry means that consumption of the good by one actor does not result in a reduced availability of said good for others. Non-excludability on the other hand refers to the practical impossibility of excluding any actors from consuming the

good (Samuelson, 1954). If benefits are shared on a global scale, public goods essentially constitute GPGs. The use of public goods usually leads to either positive or negative externalities, potentially again of a global reach.

Due to their non-rivalry and non-excludability, pure public goods face two caveats leading to under-provision (Kaul et al, 1999). The first problem is free riding, as free access to the good allows actors to benefit without contributing to availability (Boonen et al, 2019). Consequently, there are no incentives to contribute in the first place. Under these circumstances, the provision of public goods may become insufficient or even break down completely. The second is known as the prisoner's dilemma, a game theoretical paradox that adds uncertainty about the behaviour of others to the picture. In the view of incomplete knowledge, rational actors must decide whether to trust the other party and act responsibly or not. While each player prefers mutual trust and cooperation to mutual defection, the best outcome for each player is a situation in which he defects while the other side chooses to cooperate. In turn, this means that cooperating while the other player defects results in the worst possible outcome (Hansel et al, 2018). Consequently, and despite common interest, rational actors are tempted to act uncooperatively, for only by cheating can exploitation by others be avoided.

2.1 Bug Bounties and GPGs

The question remains whether cybersecurity, or more specifically BBP-generated vulnerability information, can be regarded as a GPG. Following Taddeo (2019), a system's robustness would fall under the definition, resilience and responses to attacks would not. Vulnerability information is, among other things, part of a robust system (Taddeo 2019), with Rosenzweig (2012) sharing the view and calling cybersecurity information a public good. This contrasts with commercial IT security solutions, such as anti-virus software or intrusion-detection systems, which are bought and sold on the private market and are thus excludable. The information about vulnerabilities, however, is not. Moreover, it fulfils the idea of non-rivalry as sharing with others does not reduce its usefulness to each collaborating partner.

While software vendors pay for BBPs, customers do so at most indirectly by assuming that part of the price paid for the product service is its (security) maintenance. In this way, everyone worldwide employing a specific software is benefitting from that vendor's BBP and other measures. This can be seen as a positive externality from an economic perspective. Rationally thinking, if competitor A on the market invests in secure products, it will likely attract more customers in the long run, as it develops a more sustainable product. This may lead competitor B and C to similarly invest in product security (Böhme, 2006). In view of potential misuses of computers, for example via botnets, security should rather be centred on a node as opposed to the network level (ibid.). The weakest node is likely the primary point of attack, acting as a floodgate to the whole system or network, and can therefore lead to a negative externality. In turn, a positive externality would be if one node invests in security. This way, it automatically reduces the likelihood for others to be attacked via that node's previously closed gates.

Hence, although investing in BBPs might only directly benefit own customers, it has a positive spillover effect on users of other software, too. This indirect benefit qualifies the information on vulnerabilities (resulting from BBPs) for being non-excludable while at the same time being non-rival. However, and following Weber (2017), it ultimately depends on policy choices whether vulnerability information is shared or retained by companies and governmental agencies. Stemming from this, different countries choose different strategies in governing vulnerability information.

3. Empirical Case Studies

In the following, two empirical case studies serve the purpose of inductively exploring real-word variance of BBP policies. Case selection was driven by data availability and the benefit of analysing most unlike regulatory frameworks, i.e. a focus on recent European and Chinese public policy decisions. At the same, they are of considerable intrinsic importance, given the respective market sizes.

3.1 China

On June 1, 2017, the "Cybersecurity Law of the People's Republic of China" (中华人民共和国网络安全法), commonly referred to as the Chinese Cybersecurity Law, came into effect (Creemers, Triolo, and Webster, 2018). Its Article 26 states that the publishing of vulnerabilities and other cybersecurity information "shall comply with relevant national provisions" (ibid.) and there are signs that China has been exerting pressure on its security researchers. International concerns grew when China announced not to send any security researchers to the Canadian

hacking competition 'Pwn2Own' in March 2018 (Krahulcova, 2018). A year later, in 2019, the first Chinese vulnerability disclosure regulation draft was released, requiring vulnerabilities to be reported exclusively to state authorities in a first step (Udemans, 2019). In July 2021, the Cyberspace Administration of China (CAC) issued the "Regulations on the Management of Network Product Security Vulnerability" (网络产品安全漏洞管理规定) coming into force only two months later (CAC, 2021). While its Article 7 encourages the creation of BBPs, it also establishes the state as the dominant gatekeeper on vulnerability information (Cimpanu, 2021). Thus, vendors are obligated to notify the Ministry of Industry and Information Technology (工业和信息化部) within 48 hours regarding any reported vulnerabilities. Article 9 goes even further, essentially preventing any Chinese security researchers from cooperating with (non-vendor) BBPs as they are no longer allowed to disclose vulnerability information to "overseas organizations or individuals other than network product providers" (ibid.).

These new regulations and decisions by the Chinese government send a twofold signal. First, it seems that China is free riding on the efforts of international BBPs. This does not mean that there are no Chinese efforts in setting up own BBPs or hacking competitions, as the examples of Huawei (Whittacker, 2019) or the 2021 Tianfu Cup show. Chinese BBPs make use of the global crowd of security researchers to secure their own software products. At the same time, the government does not allow its own citizens to participate in foreign BBPs. This will have a significant impact on the BBP market, according to HackerOne (2020), as Chinese security researchers are second in reporting vulnerabilities in terms of bounty in-flow.

The second and even more important element arises from the previously discussed prisoner's dilemma innate to the governance of GPGs. Given that an increasing number of states not only invest in defensively orientated security measures but also in offensive capabilities (Herpig, 2018), state security agencies have an interest in exploiting vulnerability information instead of sharing them with third parties. Here, Zero-Day Exploits (ZDE) are particularly sought after, which refer to a vulnerability that is yet unknown to the developer or vendor but exists 'in the wild'. China appears to be leaning towards this direction, having also assigned ZDEs a strategic value (O'Neill, 2021; Hewage and Ukwandu, 2021). The stockpiling of ZDEs results in even greater distrust, in turn acting as a motivator for other actors to also withhold information.

Drawing on the simplified (two-player) representation of the prisoner's dilemma, the situation could be depicted as in the table below. The most desirable outcome for international security would be a BBP market open to all vendors and security researchers where gained vulnerability information is disclosed responsibly to all parties (top left). However, recent signals sent from China indicate that it decided to put national security interests first (Thorne and Hoffman, 2021) and to move vulnerability disclosure from a GPG towards a club good, only available to vendors and the state within its borders.

		Actor A	
		Disclosure	**Retention**
Actor B	**Disclosure**	Responsible vulnerability disclosure in both states	Responsible vulnerability disclosure in State B, retention thereof in state A
	Retention	Responsible vulnerability disclosure in State A, retention thereof in state B	Both states withhold vulnerability information

One could now argue that there is nothing new about this dynamic because numerous governments around the world withhold vulnerabilities under certain circumstances, and the relevant procedures and criteria for this are also evident in many cases through so-called Vulnerabilities Equities Processes (VEPs). There is, however, a crucial difference between for example the US VEPs and the new Chinese regulations. While VEPs only decide on vulnerabilities discovered by government agencies, the Chinese government also secures access to those by third parties. Although the information is due to be shared with manufacturers as well, state intelligence services

or other government actors will have a comfortable window of opportunity to exploit reported vulnerabilities. The reason for this is the average time required for the development, testing, and distribution of patches before any effective defence can be in place. To underline this argument, consider the difference between the 30, 60 or even 90 days granted to software vendors by most BBPs prior to details being publicly released, and the maximum 48-hour time lag after which reports have to be shared with the Chinese government. Arguably, this leaves at least almost a month for exploits to be developed and used by Chinese intelligence, military, or other agencies.

Against this backdrop, Chinese BBP nationalisation and the associated withholding of vulnerability information has serious implications for international security and governance that go beyond the programs as such. On the one hand, the nationalisation of white hats will likely be seen as a threatening move to expand China's 'cyber arms arsenal', which might lead to no fewer destabilising countermeasures. On the other hand, forcing Chinese security researchers to withdraw from transnational BBPs arguably undermines the effectiveness of a transnational bottom-up mechanism of 'proliferation control' in cyberspace (Silomon, 2020).

3.2 The European Union

Popularity of OSS has skyrocketed, among not only public authorities and businesses but also individuals. In their main form, OSS licenses allow software to be freely used, modified, and shared. In many cases, development is often community-based (Berlinguer, 2020). While the responsibility to update and further develop commercial software lies with the vendor, OSS maintenance responsibility is not as clearly assigned. Often security measures including post-release bug hunting, reporting, and/or patching, are left to individuals or groups on a voluntary basis lacking financial reward structures. Given OSS development nature and often lack of revenue, it is not surprising that resources are scarce (Rogowsky, 2014). For the same reason, OSS projects cannot compete with commercial software vendors on the BBP market.

Under-protection therefore represents a classical example of market failure, where lack of incentives to invest in security leads to under-provision of (OSS-specific) vulnerability information as a GPG. While a number of private initiatives such as the Core Infrastructure Initiative and Google's Project Zero seek to address this problem, the EU launched its own hands-on solution in 2015. Its Free and Open Software Auditing (EU-FOSSA) project started with an initial one million Euro budget (European Commission, 2020) focussing on auditing two critical software programmes and running a cybersecurity awareness campaign. After its completion, EU-FOSSA 2 was launched with a wider scope in 2019. This iteration encompassed a greater number of European institutions, research on OSS use among public administrations worldwide, and, most importantly, fifteen BBPs as well as three hackathons. A core aim was to mitigate the under-provision of OSS security by creating a BBP that could match the rewards offered by commercial BBPs on the market.

Nonetheless, there is also an industrial policy rational for the EU's efforts as OSS can guarantee independence from foreign commercial software providers. Furthermore, publicly financed BBPs could support the entrance of European competitors to the current US dominance on the global BBP market (HackerOne, 2020). There have been calls for Europe to catch up and act as a counterbalance (Schulze, 2019), seeking to encourage more European-based firms to invest in crowdsourced security. In turn, this could improve European sovereignty in terms of vulnerability information and prevent foreign intelligence services gaining access or misusing the information. YesWeHack, founded in 2013, serves as a good example for a growing European stake, having grown by 450% in venture capital funding between 2019 and 2021, while security researcher participation has risen by 350% (YesWeHack, 2019 and 2021).

4. A Preliminary Theory of Regulatory Models

Both case studies illuminate ways of complementing, if not replacing, the existing primarily market-driven BBP environment. In very simplified terms, this results in a total of three models, or ideal types, for BBP and security research regulation, thus mirroring the development within other areas of internet and cybersecurity governance, such as data privacy (Aho and Duffield, 2020; Siebert, 2021). In the following section, we further elaborate on these models by offering a theoretically informed comparison of their guiding principles, diffusion potential, and impact. Starting with principles and norms, an ideal-type comparison will delve into the following characteristics:

1. The first model, emerging within the Chinese context, follows the principles of digital authoritarianism and absolute state sovereignty, and applies them to the governance of BBPs. National governments,

accordingly, have a right and duty to effectively control and capture any security research on ICT vulnerabilities within their jurisdiction, including the enabling intellectual and material resources.

2. The second model is diametrically opposed to the first, trusting essentially the market with almost all governance issues, especially as they relate to allocation of resources and the distribution of benefits. The role of the government instead is limited to making sure that an enabling legal framework is in place, for example regarding the protection of security researchers from arbitrary claims for damages. Beyond that, the government uses BBPs only for the security of its own systems.
3. Finally, European public funding of BBP on OSS may well be regarded as the nucleus of a paradigmatic middle ground, where a majority of BBPs depends on the market, but public spending is used to strategically correct for market failures and to ensure that the benefits of vulnerability research are as equally distributed as possible.

Currently, the impact of each of these models on peace and security is undoubtedly speculative, and only practical experience will show whether certain opportunities or risks materialise. Nonetheless, it is likely that the second model will result in at least some under-provision of GPGs, neither preventing free riding and thus insufficient resource allocation, nor safeguarding against misallocation, i.e. a mismatch between funding priorities and actual areas of particular concern. Furthermore, critics point out that some companies use BBPs to pressure security researchers into non-disclosure-agreements. Others use these platforms as a cheap and less demanding alternative to setting up proper vulnerability disclosure processes themselves (Porup, 2020). In both cases, use of BBPs essentially prevents rather than produces the disclosure of vulnerability information as GPG. The European effort, in contrast, while being capable of closing crucial protection gaps at the regional level, does not provide a solution to the equally challenging use of unlicensed, and therefore mostly unpatched, software. To maximise the European model, it is therefore vital to complement it with measures promoting OSS use in many countries.

Assessing the impact on peace and security of the first model, in comparison, appears straightforward. After all, the transformation of BBPs, leading to the shift of vulnerability information from a global public into a club good, with state authorities as the central gatekeeper, is certainly regrettable by systematically taking away protection from internet users and organisations worldwide. Even if there is no or only limited intention to use vulnerabilities, the mere knowledge of the nationalisation of vulnerability research exacerbates the international security dilemma and will thus probably fuel the ongoing militarisation of cyberspace. Even if the Chinese government was to publicly declare that reported security vulnerabilities would not be used for state operations, this would not change. The main reason is that this cannot be verified externally, exemplifying structural dynamics of the prisoner's dilemma discussed above.

Whatever their impact on peace and security, emerging models of regulating BBPs will matter even more when they diffuse beyond national borders, through emulation or by sanctioning others for not adopting such standards. As has been already indicated, these models mirror competing governance paradigms within related policy areas in many ways, such as the regulation of free speech or data privacy. However, as these rivalries have progressed further, they might hold some insights that could be applied to the case of BBPs and vulnerability disclosure regulation. For example, it has often been said that the "Brussels effect" (Bradford, 2021), i.e. the size of the European single market amongst other issues, is the reason that EU data protection policies are influential at the global level despite the dominance of US, and increasingly Chinese, internet companies. Thus, being able to deny or provide access to costumers can outweigh the lack of production capacities in this particular regulatory competition. Yet here, the case might be different as customers in this context are not European internet users, but the internet companies and software vendors themselves. Nevertheless, the possibility remains that others will follow the European model because of its perceived benefits or legitimacy in comparison to alternative forms.

A final characteristic of competition is that internet governance paradigms can only coexist with each other to a limited extent, as they each generate extraterritorial effects that cause conflicts at the international level (Internet Society, 2018). Governance of BBPs is likely no exception in this regard, and one such effect has already been mentioned, i.e. a reduction of available human resources within Western BBPs as the result of the forced withdrawal of Chinese security researchers. There are likely many others and additional research is needed to be able to anticipate such effects, which in themselves can be drivers of international conflict and mistrust.

5. Conclusion

Based on the growing financial volume and the increasing prevalence of BBPs worldwide used to disclose information on vulnerabilities, our paper focused on the question to what extent such bottom-up mechanisms can be understood as a contribution to global cybersecurity and thus to peace and security in general. Using the theory of GPGs, we differentiated existing practices as well as emergent regulatory models that compete with the non-commercial and apolitical original model. While commercial BBPs already dominate the field, regulatory approaches in China and the EU underline a growing trend of politicisation and state intervention. The future effects of these models on the availability of vulnerability information are foreseeably very different.

However, more research is needed to come to a more reliable conclusion in this regard and to enable adequate policy responses to possible unintended effects. First, we propose systematic quantitative studies to test deductive assumptions about the specific benefits of BBPs for peace and security with robust empirical data. Of particular interest is the extent to which the profile of vulnerabilities exploited in the context of particularly disruptive cyberattacks matches the typical characteristics of vulnerabilities discovered and reported through BBPs. The more plausible such matches are, the more this would suggest that BBPs could indeed make a significant contribution to the prevention of serious cyber incidents. While studies on the overlap between vulnerabilities used by APTs and information included within state-provided vulnerability databases in Russia and China already exist (see Leyden, 2018), the authors of this paper themselves are currently preparing a comprehensive research design particularly on BBPs.

Second, future qualitative studies could trace the relative diffusion of these or other governance models to different world regions and by various mechanisms. The latter can be processes of voluntary imitation as well as incentive-based adoption of standards. Finally, the role of transnational processes of norm- and standard-setting in the context of intergovernmental, but also private-sectoral cooperation, such as an obligation for vendors to offer BBPs (Schulze and Reinhold, 2018) should be discussed. Overall, there is a huge potential for research on various aspects of emergent BBP governance models, ranging from underlying problems to the significance of their effects on global peace and security and their relative competitiveness in a world of diverging standards and geopolitical divisions.

References

Aho, Brett and Roberta Duffield (2020) Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China, *Economy and Society* 49(2), 187-212.

Berlinguer, Marco (2020) Commons, Markets and Public Policy: Free and Open Source Software as a Laboratory for the Information Paradigm, Transform! ePaper, January 2020. Retrieved from: https://www.transform-network.net/fileadmin/user_upload/2020-01-commons_3.pdf (accessed: 27th August 2021).

Böhme, Rainer (2006) A Comparison of Market Approaches to Software Vulnerability Disclosure. In Günter Müller (ed.) *Emerging Trends in Information and Communication Security*, Freiburg: Springer, 298-311.

Boonen, Christiaan, Nicolás Brando, Samuel Cogolati, Rutger Hagen, Nils Vanstappen and Jan Wouters (2019) Governing as Commons or as Global Public Goods: Two Tales of Power, *International Journal of the Commons* 13(1), 553-577.

Bradford, Anne (2012) The Brussels Effect, *Northwestern University Law Review* 107(1), 1-68.

Chatfield, Akemi and Chris Reddick (2017) Cybersecurity Innovation in Government: A Case Study of U.S. Pentagon's Vulnerability Reward Program. In: *Proceedings of the 18th Annual International Conference on Digital Government Research*, States Island, June 2017, 64-73. DOI: 10.1145/3085228.3085233.

Cimpanu, Catalin (17/07/2021) Chinese Government Lays out new Vulnerability Disclosure Rules, The Record. Retrieved from: https://therecord.media/chinese-government-lays-out-new-vulnerability-disclosure-rules/ (accessed: 28th August 2021).

Creemers, Roger, Paul Triolo and Graham Webster (29/06/2018) *Translation: Cybersecurity Law of the People's Republic of China* (Effective June 1, 2017). Retrieved from: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ (accessed: 28th August 2021).

Cybersecurity & Infrastructure Security Agency (CISA) (17/12/2003) Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. Retrieved from: https://www.cisa.gov/homeland-security-presidential-directive-7 (accessed: 6th October 2021).

Cyberspace Administration of China (CAC) 国家互联网信息办公室 (12/07/2021), 工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知. 工信部联网安 (2021) 66号. Retrieved from http://www.cac.gov.cn/2021-07/13/c_1627761607640342.htm (accessed: 1st September 2021).

European Commission (EC) (14/07/2020) *EU-FOSSA 2 - the EU's Open Source Cybersecurity Project Ends*. Retrieved from: https://ec.europa.eu/info/news/eu-fossa-2-eus-open-source-cybersecurity-project-ends-2020-jul-14_en (accessed: 28th August 2021).

HackerOne (2020) *The 4th Annual Hacker Powered Security Report*. The Study on the Hacker-Powered Security Ecosystem. Retrieved from: https://www.hackerone.com/hacker-powered-security-report (accessed: 28th August 2021).

Hansel, Mischa, Max Mutschler and Marcel Dickow (2018) Taming Cyber Warfare: Lessons from Preventive Arms Control, *Journal of Cyber Policy* 3(1), 44-60.

Herpig, Sven (2018) Governmental Vulnerability Assessment and Management: Weighing Temporary Retention versus Immediate Disclosure of 0-Day Vulnerabilities, Stiftung Neue Verantwortung e.V., August 2018, Berlin.

Hewage, Chaminda and Elochukwu Ukwandu (25/05/2021) A Hacking Competition May Have Given China new Ways to Spy on the Uyghurs. Retrieved from: https://scroll.in/article/995578/a-hacking-competition-may-have-given-china-new-ways-to-spy-on-the-uyghurs (accessed: 28th August 2021).

Internet Society (2018) The Internet and Extra-Territorial Effects of Laws, Internet Society Concept Note. Retrieved from https://www.internetsociety.org/wp-content/uploads/2018/10/The-Internet-and-extra-territorial-application-of-laws-EN.pdf (accessed: 5th August 2021).

Kaul, Inge, Isabelle Grunberg and Marc A. Stern (1999) Defining Global Public Goods. In: Inge Kaul, Isabelle Grundberg and Marc A. Stern (eds) *Global Public Goods - International Cooperation in the 21st Century*, Oxford: Oxford University Press, 2-19.

Krahulcova, Lucie (20/09/2018) China Tips the Scale of Global Cybersecurity by Hoarding Vulnerabilities. Retrieved from: https://www.accessnow.org/china-tips-the-scale-of-global-cybersecurity-by-hoarding-vulnerabilities/ (accessed: 28th August 2021).

Kuehn, Andreas (2018) New Paradigms in Securing Software Vulnerabilities - An Institutional Analysis of Emerging Bug Bounty Programs and Their Implications for Cybersecurity, *SSRN Electronic Journal* (1), 1 16. DOI: 10.2139/ssrn.2809862.

Leyden, John (17/07/2018) Russia's National Vulnerability Database is a bit like the Soviet Union. Sparse and Slow, The Register. Retrieved from: https://www.theregister.com/2018/07/17/russia_vuln_database/ (accessed: 29th August 2021).

Malladi, Suresh Siva & Hemang Subramanian (2019) Bug Bounty Programs for Cybersecurity: Practices, Issues, and Recommendations, *IEEE Software* 7459(c), 1 9. DOI: 10.1109/MS.2018.2880508.

Mohajan, Haradhan Kumar (2018) Qualitative Research Methodology in Social Sciences and Related Subjects, *Journal of Economic Development*, Environment and People 7(1), 23-48.

O'Neill, Patrick Howell (06/05/2021) How China Turned a Prize-Winning iPhone Hack against the Uyghurs. Retrieved from: https://www.technologyreview.com/2021/05/06/1024621/china-apple-spy-uyghur-hacker-tianfu/ (accessed: 28th August 2021).

Philippens, Henry (2012) The Future Prospects of De-alerting: Complexities and Considerations for Reducing Risk, *Nuclear Notes* 2(1), 13-24. Retrieved from: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/120529_Spies_NuclearNotes2_Web.pdf (accessed: 3rd September 2021).

Porup, J.M. (2020) Bug Bounty Platforms buy Researcher Silence, Violate Labor Laws, Critics Say, CSO Online. Retrieved from: https://www.csoonline.com/article/3535888/bug-bounty-platforms-buy-researcher-silence-violate-labor-laws-critics-say.html (accessed: 8th October 2021).

Rogowsky, Marcus (2014) Analyse zur Sicherheit von Open-Source Software. Fakultät für Informatik, Technische Universität München. Retrieved from: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2014-08-1/NET-2014-08-1_20.pdf (accessed: 2nd September 2021).

Rosenzweig, Paul (2012) Cybersecurity and Public Goods: The Public/Private "Partnership". Hoover Institution, Stanford University. Retrieved from: https://bit.ly/3AxVjD5 (accessed: 10th August 2021).

Samuelson, Paul A. (1954) The Pure Theory of Public Expenditures, *Review of Economics and Statistics* 36 (4): 387-389.

Schulze, Matthias & Thomas Reinhold (2018) Wannacry About the Tragedy of the Commons? Game-Theory and the Failure of Global Vulnerability Disclosure, in: Audun Jøsang (Hg.), *Proceedings of the 17th European Conference on Cyberwarfare and Security*, Reading 2018.

Schulze, Matthias (2019) Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik, SWP-Studie, 10/2019, Berlin: Stiftung Wissenschaft und Politik.

Siebert, Zora (2021) Digital Sovereignty - The EU in a Contest for Influence and Leadership, Berlin: Heinrich Böll Stiftung, https://www.boell.de/en/2021/02/10/digital-sovereignty-eu-contest-influence-and-leadership (accessed: 29th August 2021).

Silomon, Jantje (2020) Bug Bounties: Bottom-up Initiatives as Forms of Cyber Arms Control? In: Brian K. Payne, Hongyi Wu (eds.) *Proceedings of the 15th International Conference on Cyber Warfare and Security*, Old Dominion University, Norfolk, Virginia, 12-13 March 2020, 431-438. Reading: Academic Conferences and Publishing International. DOI: 10.34190/ICCWS.20.137.

Taddeo, Mariarosaria (2019) Is Cybersecurity a Public Good? *Minds and Machines* 29: 349-354.

Thorne, Devin & Samantha Hoffman (31/8/2021) China's vulnerability disclosure regulations put state security first. Retrieved from: https://www.aspistrategist.org.au/chinas-vulnerability-disclosure-regulations-put-state-security-first/ (accessed: 6th October 2021).

Udemans, Chris (22/11/2019) China Working on Rules to Regulate Vulnerability Disclosures. Retrieved from: https://technode.com/2019/11/22/china-vulnerability-disclosures-risks/ (accessed: 28th August 2021).

Weber, Steven (2017) Coercion in Cybersecurity: What Public Health Models Reveal, *Journal of Cybersecurity* 3(3), 173-183.

Whittacker, Zack (05/11/2019) Huawei Calls Hackers to Munich for Secret Bug Bounty Meeting. Retrieved from: https://techcrunch.com/2019/11/05/huawei-secret-bug-bounty-meeting/ (accessed: 28th August 2021).

YesWeHack (14/02/2019) YesWeHack Raises €4 Million and Plans to Disrupt Europe's Cybersecurity Market. Retrieved from: https://blog.yeswehack.com/yeswehack-news/yeswehack-raises-e4-million-and-plans-to-disrupt-europes-cybersecurity-market/ (accessed: 28th August 2021).

YesWeHack (22/07/2021) YesWeHack Raises €16 Million to Accelerate its International Expansion. Retrieved from: https://blog.yeswehack.com/yeswehack-news/yeswehack-raises-e16-million-to-accelerate-its-international-expansion/ (accessed: 28th August 2021).