# Leveraging Ethical Hacking in Russia:
# Exploring the Design and Potential of Bug Bounty Programs

Evgeniia Rudenko[a], Anastasia Gnatenko[b], Andrew Milich[c], Kathryn Hedgecock[d], Zhanna Malekos Smith[e]

[a] KU Leuven, WWU Münster, Tallinn University of Technology
[b] Diplomatic Academy of Vienna
[c] Stanford University
[d] Stanford University
[e] King's College London

**Abstract:** Our increasingly internet-connected world has yielded exponential demand for cybersecurity. However, protecting cyber infrastructure is technically complex, constantly changing, and expensive. Small organizations or corporations with legacy systems may struggle to implement best practices. To increase cybersecurity for organizations in Russia, we propose fostering a culture of ethical hacking by supporting bug bounty programs. To date, bug bounties have not had the same level of success or investment in Russia as in the United States; yet, we argue that bug bounty programs, when properly established, institutionalize a culture of ethical hacking by establishing trust between talented hackers and host organizations. This paper will first define ethical hacking and bug bounty programs. It will explore the current bug bounty landscape in Russia and the United States. Based on issues identified, we will proceed to offer a set of best practices for establishing a successful bug bounty program. Finally, we will discuss some considerations for setting up bug bounty programs in Russia.

## Introduction

As the world becomes increasingly connected on the internet, more organizations are vulnerable to malicious actors, who could compromise user data or cyber infrastructure. In Russia, there has been an exponential increase in internet usage: the percent of the population using the internet in Russia has increased drastically between 2005 (15%) and 2019 (81%).[1] A 2018 McKinsey Global Institute (MGI) study of 50 smart cities, based on the latest urban technologies available to citizens, found that citizens of Moscow enjoy digital services more than anywhere else in Europe.[2] As internet access expands rapidly, so too does demand for internet services across all sectors of the economy.

One of the great dilemmas in cybersecurity is that offering basic internet services, such as a user login, can be done with relative ease; in contrast, creating robust defensive systems to protect user

[1] "Individuals using the Internet (% of population)-Russian Federation," World Bank, accessed February 20, 2020. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=RU.

[2] "Digital Solutions for a More Liveable Future," McKinsey Global Institute, June 2018, accessed April 4, 2020. https://www.mckinsey.com/~/media/McKinsey/Industries/Capital%20Projects%20and%20Infrastructure/Our%20Insights/Smart%20cities%20Digital%20solutions%20for%20a%20more%20livable%20future/MGI-Smart-Cities-Full-Report.ashx.

data are far more challenging. The paucity of cybersecurity experts coupled with the high demand for cybersecurity drives up basic costs for expertise. In Russia, this is exacerbated by legal requirements that mandate cybersecurity experts be licensed by the Federal Service for Technical and Export Control of Russia (FSTEC).[3] These constraints bear the heaviest burden on small business and non-profit organizations, who cannot bring the same financial or technical resources to bear on the issue of cybersecurity. Given this dilemma, and the importance of increasing global cybersecurity, we propose a creative solution that reduces the vulnerability of citizens' data by promoting a culture of ethical (also known as "white hat") hacking within Russia by encouraging the introduction of bug bounty programs.

The objective of this research is twofold. On the one hand, the authors introduce and explain bug bounty projects as an institutional practice of ethical hacking that could help support various types of organizations. Additionally, this paper outlines the legal and organizational barriers to implementing this particular practice of ethical hacking in Russia and suggests a way forward to institutionalizing ethical hacking in the form of bug bounty practices based on experiences in a robust bug bounty environment in the United States.

## Definitions - Ethical Hacking & Bug Bounties

***Ethical hacking*** (also known as "white hat hacking") is a term used to describe hacking behavior that is conducted without malicious intent with the purpose of disclosing vulnerabilities before they can be exploited by malicious actors. Businesses with proper resources often codify ethical hacking with a specific cybersecurity expert in a contractual arrangement known as a penetration test, or *pen testing*. However, pen testing is not all-encompassing of ethical hacking and still requires large financial resources. Rather, we propose the introduction of *bug bounty* programs.

***Bug bounty programs*** establish a medium for vulnerability disclosure direct to source and provide a financial or material reward for the disclosure of vulnerability.[4] A bug bounty is distinguished from a general vulnerability disclosure program (VDP) because it provides specific institutional framework and incentives for disclosure. A successful bug bounty program clearly outlines which hacking is permissible by designating the left and right limits of appropriate hacking. Bug bounty programs rely on the technical expertise of a community of hackers without requiring the resources to contract a pen tester. Furthermore, while penetration testing may require companies to pay a fixed price (frequently in the tens of thousands of dollars), bug bounties offer rewards proportionate to the severity of vulnerabilities discovered.[5]

Ethical hacking is a productive outlet for hackers who want to utilize their skills for the betterment of society with reduced legal risk. For this reason, bug bounty programs are often viewed in the

[3] Vyacheslav Khayryuzov, "Russian Federation: Privacy and Cybersecurity in Russia," *Mondaq*, October 31, 2018, accessed February 14, 2020. http://www.mondaq.com/russianfederation/x/750216/Data+Protection+Privacy/Privacy+And+Cybersecurity+In+Russia.

[4] "The Internet Bug Bounty," HackerOne, accessed February 20, 2020. https://www.hackerone.com/internet-bug-bounty.

[5] Forrester, *The Total Economic Impact of HackerOne Challenge:Improved Security and Compliance*, May 2019. https://www.hackerone.com/resources/reporting/total-economic-impact-study-hackerone.

context of ***crowdsourcing cybersecurity expertise,*** which allows cybersecurity professionals as private actors to contribute to ensuring the cyber resilience of information system infrastructures in organizations. For a textbook-raised cybersecurity specialist it is difficult to live the experiences and motivations of actual hackers, but "white hat hacking" gathers professionals for detecting vulnerabilities from the "hacker's perspective".[6] Gathering, or crowdsourcing, cybersecurity expertise in this respect has been attempted by different types of private and public organizations and has taken place in various forms and through various channels. These tools include, but are not limited to, public-private partnerships for cybersecurity, "govhack" hackathons,[7] and bug bounty programs, which are highlighted in this paper.[8]

Previous research has explored crowdsourcing of cybersecurity expertise through the lens of ethical hacking, with bug bounties being one of the tools for cybersecurity crowdsourcing practice. Establishing a bug bounty program deals with the peculiarities of ethical hacking culture, which is built on trust with all parties involved, as highlighted in the following section.

## Credible Commitments and a Culture of Trust

The success of a bug bounty program relies centrally on the basis of trust between the hacker and the organizing entity. The hacker must trust that the organization will not pursue legal action against them and trust that they will be rewarded for disclosing vulnerabilities according to established rules. Likewise, the organizations must trust hackers to report the vulnerabilities and follow the designated boundaries of the program.

Because the hacker and the sponsor do not form a long-term commitment (i.e. are not bound by iterated plays), a game theoretic framework would suggest bug bounties create an environment prone to defection. Reputational costs are already a major incentive for the businesses sponsoring bug bounty programs. Once the business has a reputation for not upholding the reward structure, hackers tend to use open source internet forums to notify fellow white hat hackers. However, hackers do not have the same reputational costs associated with failing to uphold their end of the program because their identities tend to stay anonymous until they submit a vulnerability.

One potential solution to this is to require the registration of hackers; however, this simultaneously may deter talented hackers who prefer to keep their identity private out of concern that they may be recruited by state agencies or falsely accused of violating established rules. Ultimately, fostering a culture of ethical hacking in Russia could be best supported by creating a legal framework that makes the bug bounty program credible.

[6] Akanksha Bansal and Monika Arora, "Ethical Hacking and Social Security," *Radix International Journal of Research in Social Science* 1, no. 11 (2012): 1-16.

[7]Kiev Gama, "Crowdsourced Software Development in Civic Apps- Motivation of Civic Hackathon Participants," *Proceedings of the 19th International Conference on Enterprise Information Systems*, 2017.

[8] Raphael Bossong and Ben Wagner, "A Typology of Cybersecurity and Public-Private Partnerships in the Context of the EU." *Crime, Law and Social Change* 67, no. 3 (2016): 265–288.

A foundation of trust and credibility among ethical hackers and organizations can be advanced by defining the rules for setting up a bug bounty program, whether within an organization or in a broader societal environment. Defining the rules of the game for ethical hacking takes a step forward towards institutionalizing this practice. The nature and the meaning of these rules are further discussed in the following section.

## Bug Bounty Requirements for Institutionalizing Ethical Hacking

Since cybersecurity vulnerabilities in IT-infrastructures at any level represent a vital threat to national security of any country, building cyber resilience should be understood in terms of a "cybersecurity triad":[9]

> "The first leg is intergovernmental, which is defined both in terms of federal interagency relationships and in the layers of relationships between the federal government and state and local governments. The second leg is public-private in terms of government to private business and critical infrastructure relations. The final leg is integrating the general population into this endeavor".[10]

Through constructing this triad, researchers highlight the complexity of protecting infrastructures and propose involving a wider range of cybersecurity experts in building digital resilience. With regard to bug bounty programs and ethical hacking, such a framework of delivering cybersecurity appears to be highly appropriate, since it justifies the need for crowdsourcing professional experiences and motivation to participate. The "cybersecurity triad" suggests that the government should play a crucial role in fostering appropriate legal, social, and ethical environments for developing robust cybersecurity solutions and institutionalizing cooperation between the hacking community and organizations of all levels.[11]

Attempts to institutionalize ethical hacking in the context of crowdsourcing cybersecurity expertise began in the 1990s, when major software companies offered beta testing of new software to selected groups of customers, offering privileged access to their products as a reward.[12] Moreover, business models have been developed, based on offering penetration testing or "ethical hacking" through controlled simulated attacks as a service. Lastly, institutionalized ethical hacking measures are often connected to "hacking contests," which are offered to a wider circle within the hacking community.[13] "Incorporating externally acquired vulnerability information" in the form of bug

[9] Richard J. Harknett and James A. Stever, "The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen," *Journal of Homeland Security and Emergency Management* 6, no. 1 (2009): 1-14.

[10] Ibid., 2.

[11] Akemi. T. Chatfield and Christopher Reddick, "Cybersecurity Innovation in Government: A Case Study of U.S. Pentagon's Vulnerability Reward Program," *Proceedings of the 18th Annual International Conference on Digital Government Research*, (June 2017).

[12] Bryan Smith, William Yurcik, and Daniel Doss, "Ethical Hacking: The Security Justification," in *Ethics and Electronic Information*, ed. Barbara Rockenbach and Tom Medina (United States: McFarland & Company, 2001), 148-151.

[13] Ibid.

bounty is a relatively new development in this area, which on a larger scale leads to a "shift in the cybersecurity paradigm" in general.[14]

Studying this issue from the institutional perspective, Kuehn and Mueller (2014) have outlined the following requirements to bug bounty measures:

1. Bug bounty practices should be based on "*explicit procedures*, which allow for straightforward, standardized forms of interactions";
2. "*Technical specifications* that describe technical and formal requirements, such as the type of bugs that are eligible under a BBP" should be captured and communicated properly to the hacker community;
3. A bug bounty program should be "governed by *terms and conditions* with regard to its structure and scope; they determine the types and sizes of bounties and stipulate rules for concurrent submission of the same bug";
4. "*Acknowledgment and reputation* are important motivational elements, such as a 'Hall of Fame' of contributors, to engage talented security researchers". [15]

The requirements proposed by Kuehn and Mueller are not intended to limit the organization of bug bounty programs to a specific legal or sectoral context. In fact, bug bounty programs may still be organized in the form of a *public-private partnership* (for example, similar to bug bounty programs offered by US government agencies) or *competitions* that can be publicly and privately hosted. Bug bounties can vary in the degree of structure of vulnerability documentation and the type of rewards announced for participants of the program or competition. These requirements offer a concrete institutional framework for bug bounty practices, which might otherwise lead to adverse consequences for organizations and in some cases for hackers themselves. Compliance with these requirements in specific environments is demonstrated in the following sections.

## Organizational Programs and Requirements for Bug Bounties

Given the financial incentives for businesses to secure their data, multiple organizations offer guidance and support for companies and governments interested in offering bug bounties. HackerOne – which offers a variety of cybersecurity services, including penetration testing – brands their program as a "hacker-powered security platform" that may yield cost savings and better compliance.[16] In 2016, HackerOne published an overview document "How to Run a Bug Bounty Program" that provides an overview of the programs' benefits, cost estimates, and suggested tips for working with the hacker community.[17] Notably, some sections of the guide presume organizations have access to well-organized engineering teams with issue-tracking software (such as Jira). Key insights from the guide include suggestions for progressively

[14] Andreas Kuehn and Milton Mueller, "Shifts in the Cybersecurity Paradigm: Zero-day Exploits, Discourse, and Emerging Institutions," *Proceedings of the 2014 New Security Paradigms Workshop* (September 2014): 63-67.

[15] Ibid.

[16] "Hackerone - About," HackerOne, accessed January 18, 2020. https://www.hackerone.com/about.

[17] "How To Run A Bug Bounty Program," HackerOne, accessed January 21, 2020. https://www.hackerone.com/lp/node/1016.

increasing a bug bounty program's scope (such as from private, invited hackers to the general public) and considerations for when and how to pay hackers.

Individual cybersecurity researchers have also published articles outlining steps towards running a robust and useful bug bounty program. In one article entitled "A Comprehensive Guide to Running a Bug Bounty Program," security engineer Julian Berton provides additional steps towards offering bug bounties that could prove useful for the social sector.[18] He suggests that organizations begin by setting up Vulnerability Disclosure Programs (VDPs) to solicit bug and vulnerability reports. Acknowledging the potential legal concerns associated with finding or exploiting vulnerabilities, the US Department of Justice released an additional step-by-step guide to manage technical and legal risk, such as prosecution under the U.S. Computer Fraud and Abuse Act (CFAA). [19]

Other security researchers have offered additional guidance on how the CFAA and other laws, such as Europe's General Data Protection Legislation (GDPR), impact bug bounty programs. The CFAA outlaws accessing "a computer without authorization" or obtaining "information from any protected computer." Although the CFAA was enacted in 1986 to prevent malicious hacking, it has been widely criticized as "draconian" and "outdated" by mandating severe penalties for infractions. While CFAA, as intended, prohibits intentionally accessing a computer system without proper authorization, it does not clearly define the critical term "without authorization" and instead mandates that the perpetrator be punished by either a fine or imprisonment.[20] This ambiguity has led to much criticism of the statute and to a call for reform amongst the policy and technology communities.[21]

Generally, legislation's poor definition of "unauthorized access" has become antiquated, particularly in the context of bug bounty programs where non-employees may access a company's servers. Cybersecurity companies, including HackerOne, have published articles analyzing how bug bounties and VDPs can be enacted while still respecting the CFAA; generally, articles written by lawyers suggest that the concept of "consent" from an organization in VDP or bug bounty program is critical. However, the severe penalties associated with CFAA prosecution may deter hackers from wanting to participate, particularly if bug bounty programs are initiated with significant technical restrictions around the type of vulnerabilities that can be exploited.

The GDPR has a more nuanced impact on the risks associated with bug bounty programs. The GDPR was enacted in 2018 to protect the privacy and security of personal data of individuals in the European Economic Area (EEA) and select non-EEA entities that handle the personal data of

[18] Julian Berton, "A Comprehensive Guide to Running a Bug Bounty Program," *Medium*, January 4, 2019, https://medium.com/@berton.julian/part-5-a-guide-to-running-a-bug-bounty-program-71a829f90f94.

[19] Ibid.

[20] 18 U.S. Code § 1030. https://www.law.cornell.edu/uscode/text/18/1030.

[21] *Computer Fraud and Abuse Act*, The National Association of Criminal Defense Lawyers, accessed February 12, 2020, https://www.nacdl.org/Landing/ComputerFraudandAbuseAct.

subjects in the EEA.[22] Pursuant to GDPR Article 4 (1), personal data is defined as: "Any information which is related to an identified or identifiable natural person."[23] Thus, bug bounty programs that could lead organizations or white-hat hackers to expose or access identifiable information could lead to liability under the GDPR. This establishes a Catch-22: by offering bug bounty programs to identify that data, organizations may unearth critical vulnerabilities that yield better GDPR compliance and security for personal data. Guidance, such as from the secure-software storage firm Egnyte, suggests that poorly managed bug bounty programs could lead to unintentional GDPR violations. For example, a hacker could post screenshots or documents to prove the existence of a vulnerability that inadvertently releases users' personal information. These technical requirements, international legal frameworks, and potential areas of liability provide context for analyzing the past and present bug bounty environment.

## Mapping the Current Bug Bounty Environment

Due to the legal and technical barriers discussed in the previous section, the earliest organizations in the US to offer financial incentives for ethical hacking were fast-growing internet companies, including Netscape, Mozilla, Google, Facebook, and others.[24] As the private sector successfully implemented such programs, US government agencies took notice. In 2016, the Department of Defense (DoD) launched the federal government's first bug bounty program called "Hack the Pentagon" to crowdsource vulnerabilities in the DoD's "public facing systems."[25] Over 8,000 vulnerabilities were reported. In 2018, the DoD expanded the program and issued contracts to three private sector cybersecurity firms – HackerOne, Bugcrowd, and Synack – to further incentivize ethical hacking and leverage a distributed network of cybersecurity expertise for national security.

In addition, the Federal Trade Commission (FTC) and Department of Justice (DoJ) are pushing companies to provide a means for good-faith security researchers to report bugs and put effective processes in place to act on those reports. The FTC has recommended that companies have an ongoing process to keep up with security practices as threats, safety hazards, technologies, and business models evolve. This involves at least two components. First, companies should take steps to stay abreast of threats identified in the marketplace by, for example, signing up for email updates from trusted sources, checking free databases of vulnerabilities identified by security researchers, and maintaining a channel through which security researchers can reach out about risks. Indeed, in many cases, the FTC has alleged, among other things, that failure to maintain an adequate process for receiving and addressing security vulnerability reports from security researchers and

[22] *The European Union (EU) General Data Protection Regulation (GDPR),* University of Pittsburgh. http://www.irb.pitt.edu/GDPR "The following countries have adopted the GDPR at the time of this writing and make up the EEA: Austria, Belgium, Bulgaria, Croatia, the Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Swede, the United Kingdom, Norway, Iceland, and Lichenstein."

[23] "General Data Protection Regulation," Article 4 (1), accessed February 8, 2020, https://gdpr-info.eu/.

[24] Esben Friis-Jensen, "The History of Bug Bounty Programs," *Cobalt.io*, April 11, 2014, https://blog.cobalt.io/the-history-of-bug-bounty-programs-50def4dcaab3.

[25] "Department of Defense Expands 'Hack the Pentagon' Crowdsourced Digital Defense Program." United States Department of Defense, accessed April 2020. https://www.defense.gov/Newsroom/Releases/Release/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/.

academics is an unreasonable practice, in violation of Section 5 of the FTC Act.[26] Official endorsement of this kind creates momentum for bug bounty programs in the US.

In Russia, despite a lack of attention to bug bounty programs, there is still a robust hacking culture. Ethical hacking is not an entirely foreign concept. Since 2011, Positive Technologies has been hosting one of Russia's largest ethical hacking conferences in Moscow, the Positive Hack Days Conference.[27] Additionally, some hacking schools within Russia emphasize the importance of ethics in hacking.[28]

Despite an awareness of white hat hacking, existing bug bounty programs in Russia are sparse. As of February 2020, HackerOne had only eight active bug bounty programs associated with '.ru' domain names. One enterprise that has ventured into the bug bounty space is Kaspersky Lab, a Russian-based global cybersecurity provider headquartered in Russia.[29] They introduced their bug bounty program in 2016 and increased the size of the maximum reward to $100k in 2018. Another notable entry into the bug bounty culture is Yandex. Yandex is the largest technology company in Russia and has recognized the value of crowdsourcing cybersecurity.[30] However, there are reports in some online hacking communities that Yandex has not upheld their end of the bargain by making good on rewards for tips. Hackers have become frustrated by what they see as fixed exploitations, without receiving payment for their disclosure.[31] This fundamentally erodes a culture of ethical hacking by reducing the credibility of disclosure. It is a risky gamble for a business to withhold or refuse to honor the rewards promised; once a company has established a bug bounty, they are inviting probes into their network, but a hacker does not have incentive to report vulnerabilities if the sponsoring entity has a reputation to be untrustworthy.

When it comes to official endorsement for VDPs in Russia, there is a lack of cybersecurity initiative when compared with parallel developments in the US. Many cybersecurity activities in Russia are concentrated in the public sector, more precisely in intelligence gathering. In May 2016, Deputy Minister of Communications, Alexei Sokolov, suggested that the Russian government was mulling over the possible implementation of bug bounty programs to improve cybersecurity. However, there was little follow up to this public statement.[32] The Ministry of Digital

[26] "Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection," June 15, 2018 https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-federal-trade-commissions-bureau-consumer-protection-consumer-product-safety/p185404_ftc_staff_comment_to_the_consumer_product_safety_commission.pdf.

[27] Patrick Reevell, "Inside One of Russia's Largest Hacking Conferences," ABC News, May 17, 2018. https://abcnews.go.com/International/inside-largest-hacking-conferences-russia/story?id=55201815.

[28] Alexander Osipovich, "Inside a Russian Hacker School," *Foreign Policy*, October 12, 2009. https://foreignpolicy-com.stanford.idm.oclc.org/2009/10/12/inside-a-russian-hacker-school/.

[29] "Kaspersky Bug Bounty Program," HackerOne, accessed February 2020. https://hackerone.com/kaspersky.

[30] "Yandex, Russia's biggest technology company, celebrates 20 years," *The Economist,* September 30, 2017, https://www.economist.com/news/business/21729779-search-giant-thriving-faces-political-pressures-yandex-russias-bIggest-technology.

[31] Neal Poole. "Experiences With the Yandex Bug Bounty Program," April 16, 2013, https://nealpoole.com/blog/2013/04/experiences-with-the-yandex-bug-bounty-program/.

[32] Vladimir Zykov, "Ministry of Communication will attract hackers to search for vulnerabilities in the Russian soft." Izvestia. May 25, 2016. https://iz.ru/news/615406.

Development, Communications and Mass Media of the Russian Federation mentioned bug bounties as a good way "...to stimulate research in the field of vulnerability detection, learning from international experience".[33] Our research indicates that the Russian government never formally introduced public-facing bug bounty programs. The only example identified was a public testing of the e-voting system in 2019 for the Moscow City Duma elections.[34]

### Recommendations for Developing Bug Bounty Programs in Russia

Existing literature suggests that daunting compliance, technical, and organizational requirements exist in initiating a bug bounty program, from having an engineer "on-call" to triage issues to carefully assessing compliance under CFAA, GDPR, and other forms of legislation. Therefore, based on the issues addressed in this paper, we suggest a list of primary recommendations for organizations in Russia that could benefit from bug bounty programs. These contain some of the most important legal, organizational, and technical considerations helping organizations lay the groundwork for utilizing the benefits of crowdsourced cybersecurity expertise in the form of bug bounties.

We start by providing the list of **general obligations for data handlers** under the Personal Data Law (152-FZ), composed by Vyacheslav Khayryuzov, head of data privacy at Noerr LLP.[35] The law applies to most data operators in Russia, however, the exact list of measures is defined on a case-by-case basis. Relevant measures may vary depending on the types of data collected and the means of collection and processing.

Data handlers must:

- Collect the consent of data subjects – consent should be required to be collected and, in certain cases, be in writing (ink on paper) unless certain exemptions are clearly applicable;
- Check the country of the data recipient in the event of cross-border transfers, since an additional authorization for transfers to certain countries may be necessary;
- Have a data transfer agreement for any third-party transfers;
- Have a primary database in Russia for personal data of Russian citizens;
- Comply with technical requirements of the FSB (Federal Security Service) and FSTEK (Federal Service for Technical and Export Control of Russia), as well as Decree No. 1119;
- Perform an internal data protection audit once every three years;
- Adopt internal regulations on personal data protection and a privacy policy;
- Appoint a data privacy officer;
- Handle requests of individuals;
- Define potential threats to personal data subjects;
- Acquaint employees with the internal data protection processes and regulations, and conduct training sessions on personal data security; and

[33] Ibid.
[34] "You Can't Hack: Programmers will test the reliability of electronic voting," Official website of the Mayor of Moscow. https://www.mos.ru/news/item/58866073/.
[35] Vyacheslav Khayryuzov, "Russia" in *The Privacy, Data Protection and Cybersecurity Law Review, Sixth Edition*,ed. Alan Raul (October 2019), https://thelawreviews.co.uk//digital_assets/a3cf7f19-36b0-4627- 84fe-805c58ab9ae7/The-Privacy-Data-Protection-and-Cybersecurity-Law-Review-Edition-6-secured.pdf.

- Register with the DPA (unless subject to exemptions).[36]

All in all, fulfilling the requirements of data protection regulations, both in Russia and abroad, in organizational processes and international data transfers is crucial to protecting both the hacker and the sponsoring entity within the scope of bug bounty programs. In doing so, special emphasis should be put on protecting a hacker's personal data, including name, date of birth, address of residency, and contact details. Data protection measures could be embedded in the process or IT-design of vulnerability disclosure programs in the form of storage limitations and data minimization. Having assured the security of a hacker's identity, organizations can proceed with further legal, organizational, and technical steps.

Russian organizations willing to establish bug bounty programs have two main options in terms of its maintenance. First, if there exists strong in-house expertise within an organization, it can establish an 'independent' bug bounty program, managing it without assistance from a third party. Second, if resources and technical expertise are constrained, the services of companies like HackerOne or Bugcrowd could be used to help set up a VDP and manage the inflow of issues reported. Whichever option is preferred by an organization, it is important to lay the groundwork for smooth operations. Tracing back to the framework introduced by Kuehn & Mueller (2014), establishing bug bounty programs in Russia requires further legal, organizational, and technical measures to launch bug bounties.

***Standardized Forms of Interaction.*** Achieving *straightforward, standardized forms of interaction requires a legal framework, which stipulates explicitly relevant procedures and processes of bug bounty, both inside of the organization and in a broader socio-political environment*. As of now, there is no legal framework in Russia that specifies rules for establishing bug bounty programs or VDPs. For example, acknowledging both the potential legal concerns associated with running a bug bounty program and the growing demand for cybersecurity, the US Department of Justice released a step-by-step guide to manage those technical and legal risks, such as prosecution under the U.S. Computer Fraud and Abuse Act (CFAA). This represents a best practice Russia could follow.

***Rules of Interaction.*** An organization itself needs to *establish rules that govern the interaction of ethical hackers among each other, with the bug bounty host, and within the external environment*. The lack of specialized legal guidance (like the DoJ guide in the US) means that organizations in Russia interested in establishing bug bounty programs need to put special emphasis on properly setting up a Vulnerability Disclosure Program. VDP is essential, as it offers a secure channel for researchers to report security issues and vulnerabilities and typically includes a framework for intake, triage, and workflows for remediation.

From the legal risk perspective, the most important consideration when setting up a VDP should be the network components and data that an organization includes there. First, clear distinction

[36] Ibid., 298-299.

should be made internally between sensitive and non-sensitive network components. Secondly, if sensitive components are included (those containing user data, for example), it is essential to make sure that special handling requirements are in place (e.g. prohibiting sensitive information from being saved, stored, transferred, or otherwise accessed after initial discovery). This could help to substantially reduce the likelihood that activities described in VDP will result in a civil, administrative, or criminal violation under the Russian Federal Law on Personal Data (152-FZ).

***Technical Scope.*** Furthermore, organizations should clearly *delineate the scope of the bug bounty program, based on which channels for bug reporting and types of rewards can be defined*. As a precondition to the technical definition of a bug bounty program's scope, initial lower difficulty and risk steps for protecting computer systems should be taken into consideration by organizations. An initial step involves upgrading security protocols that browsers use to connect to an organization's online resources. Organizations may obtain and publicly register cryptographic certificates for their site, thereby allowing any visitors to a site to verify its authenticity. Given a trusted cryptographic certificate, visitors to a site may also communicate with the organization's servers in a secure manner.[37]

Organizations may also run open-source vulnerability scanners, which probe websites and servers for security flaws.[38] These tools may also test servers against denial of service (DOS) attacks, which attempt to overwhelm a server with a flood of connections. These security upgrades and open-source tools may yield critical cost-saving security improvements for organizations unable to absorb the cost and risk of private sector bug bounty programs. These steps also suggest an initial basis for ensuring security prior to exposing a bug bounty program to the public.

When these measures have been taken and the need for setting up a bug bounty program has been confirmed, organizations need to make a vital decision, based on their technical and human resources, of what kind of bugs it will be able to outsource to the ethical hackers' community at the initial stage of setting up a bug bounty program. As pointed out in the HackerOne overview document "How to Run a Bug Bounty Program", the scope can be adjusted at further stages, as organizational capacities to run a bug bounty program increase.

***Reward Program.*** Finally, organizations need to *identify appropriate means of encouragement available to them and formalize a reward program for bug bounty participants*. As mentioned previously, a reward program can include financial endorsement, reputational praise in the form of a "Hall of Fame", or a combination of both. While the reporting of various bugs does not deliver the equal cybersecurity value to an organization, it is crucial that organizations balance the value of vulnerability information with the resources available to develop a differentiated and motivating bug bounty program.

[37] "TLS Security 4: SSL/TLS certificates," Acunetix, https://www.acunetix.com/blog/articles/tls-ssl-certificates-part-4/.

[38] "OpenVAS - Open Vulnerability Assessment Scanner," *OpenVas.org*, https://www.openvas.org/.

Such emphasis should be put on the rewards program, because of the fact that ethical hacking culture is, in its essence, a culture of trust, where reward programs serve as an assurance to fulfilling the obligations of the hosting organization. Failing to demonstrate the commitment to rewarding participants, as the example of Yandex shows, may result in discreditation of the program and discourage cybersecurity experts from taking the time to support the organization.

All in all, apart from ensuring initial compliance with data protection regulation to protect ethical hackers and bug bounty hosting organizations themselves, defining standardized forms, rules of interaction, technical scope, and rewarding mechanisms are essential to setting up bug bounty programs in the Russian context. Fulfilling these requirements could ensure successful cybersecurity outsourcing and help institutionalize ethical hacking.

## Conclusion

Cybersecurity is critically important to the functioning of an increasingly digital society. However, cybersecurity expertise can be scarce and cost prohibitive. Throughout this paper, we have proposed a creative approach to widespread cybersecurity in Russia through the use of ethical hacking, particularly in the form of bug bounty programs. This paper reviewed the current existing ethical hacking landscape in Russia and the United States. It also provided preliminary considerations to best foster a culture of ethical hacking and provided cautionary concerns regarding the broader legal landscape. Ultimately, a transparent institutional framework that clearly articulates the rules and limitations of bug bounty programs would foster a necessary culture of trust among hackers and organizations and may lay the foundation for cybersecurity cooperation within ethical hacking practices.

**Bibliography**

Bansal, Akanksha and Arora, Monika. “Ethical Hacking and Social Security.” *Radix International Journal of Research in Social Science* 1, no. 11 (2012): 1-16.

Berton, Julian. “A Comprehensive Guide to Running a Bug Bounty Program.” *Medium,* January 4, 2019. https://medium.com/@berton.julian/part-5-a-guide-to-running-a-bug-bounty-program- 71a829f90f94.

Bossong, Raphael, & Wagner, Ben. “A Typology of Cybersecurity and Public-Private Partnerships in the Context of the EU.” *Crime, Law and Social Change* 67, no. 3 (2016): 265–288.

Chatfield, Akemi. T. and Reddick, Christopher, “Cybersecurity Innovation in Government: A Case Study of U.S. Pentagon’s Vulnerability Reward Program.” *Proceedings of the 18th Annual International Conference on Digital Government Research,* (June 2017).

“Comments of the Staff of the Federal Trade Commission’s Bureau of Consumer Protection,” June 15, 2018. https://www.ftc.gov/system/files/documents/advocacy_documents/comment- staff-federal-trade-commissions-bureau-consumer-protection-consumer-product-safety/p185404_ftc_staff_comment_to_the_consumer_product_safety_commission.pdf.

*Computer Fraud and Abuse Act.* The National Association of Criminal Defense Lawyers. Accessed February 12, 2020. https://www.nacdl.org/Landing/ComputerFraudandAbuseAct.

“Department of Defense Expands ‘Hack the Pentagon’ Crowdsourced Digital Defense Program.” United States Department of Defense, accessed April 2020. https://www.defense.gov/Newsroom/ Releases/Release/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/.

“Digital Solutions for a More Liveable Future.” McKinsey Global Institute. June 2018. Accessed April 4, 2020. https://www.mckinsey.com/~/media/McKinsey/Industries/Capital%20 Projects%20and%20Infrastructure/Our%20Insights/Smart%20cities%20Digital%20solutions%20for%20a%20more%20livable%20future/MGI-Smart-Cities-Full-Report.ashx.

Friis-Jensen, Esben. “The History of Bug Bounty Programs.” *Cobalt.io,* April 11, 2014. https://blog.cobalt.io/the-history-of-bug-bounty-programs-50def4dcaab3.

Gama, Kiev. “Crowdsourced Software Development in Civic Apps- Motivation of Civic Hackathon Participants.” *Proceedings of the 19th International Conference on Enterprise Information Systems*, 2017.

“General Data Protection Regulation,” Article 4 (1). Accessed February 8, 2020. https://gdpr-info.eu/.

“Hackerone - About.” HackerOne. Accessed January 18, 2020. https://www.hackerone.com/ about.

Harknett, Richard J. and Stever, James A."The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen." *Journal of Homeland Security and Emergency Management* 6, no. 1 (2009): 1-14.

"How To Run A Bug Bounty Program." HackerOne. Accessed January 21, 2020. https://www.hackerone.com/lp/node/1016.

"Individuals using the Internet (% of population)-Russian Federation." World Bank. Accessed February 20, 2020. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=RU.

"Kaspersky Bug Bounty Program." HackerOne. Accessed February 2020. https://hackerone.com/kaspersky.

Khayryuzov, Vyacheslav. "Russian Federation: Privacy and Cybersecurity in Russia." *Mondaq*. October 31, 2018. Accessed February 14, 2020. http://www.mondaq.com/russianfederation/x/ 750216/Data+Protection+Privacy/Privacy+And+Cybersecurity+In+Russia.

Khayryuzov, Vyacheslav. "Russia" in *The Privacy, Data Protection and Cybersecurity Law Review, Sixth Edition,* ed. Alan Raul (October 2019). https://thelawreviews.co.uk//digital_assets/ a3cf7f19-36b0-4627-84fe-805c58ab9ae7/The-Privacy-Data-Protection-and-Cybersecurity-Law-Review-Edition-6-secured.pdf.

Kuehn, Andreas, and Mueller, Milton. "Shifts in the Cybersecurity Paradigm: Zero-day Exploits, Discourse, and Emerging Institutions." *Proceedings of the 2014 New Security Paradigms Workshop* (September 2014): 63-67.

"OpenVAS - Open Vulnerability Assessment Scanner." *OpenVas.org*. https://www.openvas.org/.

Osipovich, Alexander. "Inside a Russian Hacker School." *Foreign Policy*. October 12, 2009. https://foreignpolicy-com.stanford.idm.oclc.org/2009/10/12/inside-a-russian-hacker-school/.

Poole, Neal "Experiences With the Yandex Bug Bounty Program." April 16 , 2013. https://nealpoole.com/blog/2013/04/experiences-with-the-yandex-bug-bounty-program/.

Reevell, Patrick. "Inside One of Russia's Largest Hacking Conferences." ABC News. May 17, 2018. https://abcnews.go.com/International/inside-largest-hacking-conferences-russia/story? id=55201815.

Smith, Bryan, Yurcik, William., and Doss, Daniel. "Ethical Hacking: The Security Justification," in *Ethics and Electronic Information*, ed. Barbara Rockenbach and Tom Medina (United States: McFarland & Company, 2001), 148-151.

"The Internet Bug Bounty." HackerOne. Accessed February 20, 2020. https://www.hackerone.com/internet-bug-bounty.

*The Total Economic Impact of HackerOne Challenge:Improved Security and Compliance*. Forrester, May 2019. https://www.hackerone.com/resources/reporting/total-economic-impact- study-hackerone.

"TLS Security 4: SSL/TLS certificates." Acunetix. Accessed March 18, 2020. https://www.acunetix.com/blog/articles/tls-ssl-certificates-part-4/.

"Yandex, Russia's biggest technology company, celebrates 20 years," *The Economist*. September 30, 2017. https://www.economist.com/news/business/21729779-search-giant-thriving-faces- political-pressures-yandex-russias-bIggest-technology.

"You Can't Hack: Programmers will test the reliability of electronic voting." Official Website of the Mayor of Moscow. https://www.mos.ru/news/item/58866073/.

Zykov, Vladimir. "Минкомсвязи привлечет хакеров для поиска «дыр» в российском софте." Izvestia. May 25, 2016. https://iz.ru/news/615406.

18 U.S. Code § 1030. https://www.law.cornell.edu/uscode/text/18/1030