AARMS Vol. 22, No. 3 (2023) 5–18.

10.32565/aarms.2023.3.1

Assessing Offensive Cyber Capabilities

Exploring the Talent Behind Cybersecurity

Gábor SELJÁN[1]

The recent emergence of mercenary spyware like Pegasus or Russia's ongoing conventional warfare in Ukraine, supplemented by a cyber offensive we never experienced before, made cybersecurity even more critical. Despite the considerable research in the field, it seems that academia and the private sector have not been able to keep up with the growing importance of security and privacy resulting from the significant increase in cyber threats to critical services, infrastructure and human rights. Research on cyber capabilities tends to focus on the general understanding of the field and pays less attention to the rapid spread of increasingly advanced offensive cyber capabilities. Correctly assessing the capabilities of others and recognising the steps necessary to develop their own capabilities are essential for any country in combating future cybersecurity challenges. However, since there is no consensus on describing even basic cyber capabilities, current research uses different interpretations and usually lacks offensive capabilities altogether. In this article, I discuss the problem of assessing, measuring and evaluating offensive cyber capabilities, starting from the different definitions of some related terms through the various cyber power indices, right down to the talent behind cybersecurity, and perhaps the most promising indicators for assessing offensive capabilities.

Keywords: *cyber power, cyber capabilities, offensive security, cybersecurity indices*

Defining offensive cyber capabilities

To date, there is no well-defined or generally agreed-upon definition of the term *cyber power.* Even the term *vulnerability* has more than a dozen definitions and formulations in the glossary compiled by the Computer Security Resource Center (*CSRC*) at the National Institute of Standards and Technology (*NIST*)[2], hence what constitutes *offensive cyber capability* (*OCC*) is even more heavily debated both in academia and among policy-makers. It is cumbersome to agree on a universal definition of offensive cyber

[1] PhD candidate, Corvinus University of Budapest, e-mail: gabor.seljan@stud.uni-corvinus.hu

[2] CSRC 2021.

capabilities for several reasons. As explained by Miralis (2019), a narrow definition may exclude so many potentially malicious offensive cyber activities that policy-making efforts based on that definition will be futile. However, a broader definition may also capture legitimate activities, for example, research and development, aiming to create the necessary cybersecurity tools to defend against cyberattacks and any limitation on those activities could harm cyber incident responders and network defenders more than threat actors.[3] In the following paragraphs, I briefly overview some of the related terms and their interpretations.

In his proposed definition, Kuehl (2009) outlined the fundamental ideas of cyber power: "*The ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power.*"[4] According to this early interpretation, cyberspace was already considered to be a domain of warfare, although NATO officially recognised it as the fifth domain of operations much later at the Warsaw Summit, as further explained by Minárik (2016).[5] Meanwhile, in the view of the Economist Intelligence Unit (*EIU*) and Booz Allen Hamilton (*Booz*), cyber power is "*the ability of a country to withstand cyberattacks and to deploy the digital infrastructure needed for a productive and secure economy*",[6] which interpretation feels somewhat controversial.

Considering the military approach to offensive cyber capabilities, for example, the military doctrine of the United States defines a cyberspace capability as *"a device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace"*,[7] while the military doctrine of both the United States and the United Kingdom defines *offensive cyber operations (OCO)* very similarly as *"activities that project power to achieve military objectives in, or through, cyberspace"*.[8] The Allied Joint Doctrine for Cyberspace Operations further discusses the military context, emphasising that, besides supporting operations in the physical domains, offensive cyber capabilities may also aid information operations *"to influence, disrupt, corrupt or usurp the decision-making of adversaries"*.[9] However, the document does not explain the term *"capabilities"* in detail. Uren et al. (2018) from the Australian Strategic Policy Institute (*ASPI*) proposed another definition, explaining that *"in the context of cyber operations, having a capability means possessing the resources, skills, knowledge, operational concepts and procedures to be able to have an effect in cyberspace"*.[10]

From these various definitions and formulations, Gunjan Chawla and Vagisha Srivastava (2020) from the Centre for Communication Governance at the National Law University Delhi (*CCG NLU*) concluded that *"cyber capabilities and cyber operations are not synonymous, but cyber capabilities are a prerequisite to conducting offensive cyber operations"*.[11] This view is further corroborated by DeSombre et al. (2021) from the

3 Miralis 2019.
4 Kuehl2009: 24–42.
5 Minárik 2016.
6 Economist Intelligence Unit 2011: 7.
7 Joint Chiefs of Staff 2018: 100.
8 Ministry of Defence 2018: 32.
9 NATO Standardization Office 2020: 25.
10 Uren et al. 2018.
11 Chawla–Srivastava 2020.

Atlantic Council's Cyber Statecraft Initiative, which defines offensive cyber capabilities as *"the combination of tools; vulnerabilities; and skills, including technical, organizational, and individual capacities used to conduct offensive cyber operations".*[12]

As explained by Christopher S. Chivvis and Cynthia Dion-Schwarz (2017), compared to the conventional methods used by nation states, offensive cyber capabilities are less expensive, more difficult to detect and attribute (or at least easier to deny), and more effective to cause the target serious harm by exploiting security flaws. Due to the asymmetrical nature of cyber capabilities, smaller or simply resource poor countries can outperform large, resource rich nations and have a greater impact in cyberspace than they would otherwise have in the physical space.[13]

Measuring offensive cyber capabilities

> *"Achievements are made by talent, and industries are expanded by talent. In all things in this world, people are the most precious; and all innovative achievements are produced by people. Hard power or soft power, when it comes down to it, it all depends on the power of talent."* – Xi Jinping, 2018[14]

How can we assess and measure something that is not clearly defined? Though notable research was published by military- and defence-related organisations, studies on cyber power are much less common than studies on cybersecurity. There are also visible attempts to evaluate a nation's cyber power capability among the studies. For example, the National Capabilities Assessment Framework (*NCAF*) proposed by Sarri et al. (2020) from the European Union Agency for Cybersecurity (*ENISA*) provides a self-assessment of the level of maturity by assessing specific objectives to help enhance and build cybersecurity capabilities.[15]

Still, comprehensive comparisons of cyber power indices and associated studies focusing on offensive cyber capabilities are lacking in the literature. To fill this void, in a recent study, Çifci (2022) analysed global indices and studies for assessing cybersecurity and cyber power and compared them in terms of their comprehensiveness and strength for measuring country-level capabilities. For this purpose, Çifci proposed a conceptual framework that classified ninety indicators into fourteen categories, one of which is offensive capabilities. The framework offers only two indicators for cyber workforce and five each for cybersecurity research and offensive capabilities. However, the comparison excludes the latter category to maintain accurate calculations.[16]

Over the past decade, several organisations have worked on creating methods to assess the cyber power of countries, according to their interpretations. Many of them have been based on data collected by self-assessment via surveys with questionnaires, often resulting

[12] DeSombre et al. 2021b: 1.
[13] Chivvis–Dion-Schwarz 2017.
[14] Murphy et al. 2021.
[15] Sarri et al. 2020.
[16] Çifci 2022.

in composite weighted indices that produce a final ranking of countries. One of the various drawbacks of such indices is that the results can only be interpreted in relation to each other and if many countries are close in score, their rankings must be interpreted with special care. Composite indices are mostly focused on cybersecurity in general, covering various aspects of the information and communication technology (*ICT*) sector, including cyber incident response and recovery. Another difficulty is that the various organisations define the concept of cyber capabilities differently and therefore also measure them differently. In the following paragraphs, I briefly summarise some of the reports associated with measuring cyber capabilities.

A study on Cyber Warfare (*CW*) created by the Institute for Security Technology Studies (*ISTS*) at Dartmouth in 2004 was one of the first and most extensive research in determining the cyber warfare capability of countries. As Çifci (2022) summarised this study in a recent paper, Dartmouth researchers used an interdisciplinary method to combine strategic, technological and political analysis to provide an evaluation of the offensive cyber capabilities of chosen nation states and the possible consequences of cyberattacks on United States computer networks. Instead of quantitative measurements or rankings, the study measures government and private sector capabilities and provides qualitative statements about the selected nations.[17]

The Cyber Power Index (*CPI*), created in 2011 by the Economist Intelligence Unit (*EIU*) and Booz Allen Hamilton (*Booz*), ranked nineteen of the G20 nations in four areas: legal and regulatory framework; social-economic context; technology infrastructure; and industry application. The *CPI* claims to provide a broad measure of cyber power because it does not solely assess cybersecurity-related capabilities. However, with little focus on defence, it emphasises the economic and resource indicators, which do not fully depict cyber power, and it does not measure or even mention offensive cyber capabilities.[18]

The International Telecommunication Union's (ITU) Global Cybersecurity Index (GCI) first published in 2015 is based on the weighted scoring of questionnaire responses received from countries participating in the survey. The GCI is a composite index of several indicators that monitor and compare the level of the cybersecurity commitment of countries regarding the five pillars of the Global Cybersecurity Agenda (GCA), including the legal, technical, organisational and capacity-building measures and the cooperation aspects of national cybersecurity cultures of different countries. The GCI is published for over one hundred seventy countries and is one of the most comprehensive measures of cybersecurity commitment of countries; however, the five pillars of the cybersecurity agenda do not cover offensive capabilities.[19]

The Cyber Readiness Index (CRI) 2.0 also published in 2015 by Demchak et al. from the Potomac Institute evaluates and measures a country's preparedness levels for certain cybersecurity risks, paying particular attention to the economic importance of cybersecurity or in other words the "economic erosion caused by cyber insecurity". Although the CRI

[17] Billo–Chang 2004.
[18] Economist Intelligence Unit 2011: 7.
[19] ITU 2021.

2.0 analyses one hundred twenty-five nations, it does not rank or score them and only briefly mentions offensive capabilities as part of defence and crisis response.[20]

The report entitled "Cyber Capabilities and National Power: A Net Assessment" published in 2019 by the International Institute of Strategic Studies (IISS) follows a qualitative methodology and analyses the wider cyber ecosystem. The CCNP represents a snapshot in time and assesses the capabilities of fifteen countries in seven categories, including offensive cyber defined as "cyber operations that are principally intended to deliver an effect rather than those principally intended to gather intelligence". Furthermore, the report considers cyber espionage and network exploitation as intelligence gathering and covers them as core cyber intelligence capabilities. The CCNP divides the actors into three tiers based on their world-leading strengths in the various categories, but it does not rank the countries under investigation numerically within the tiers, because that would depend on the degree of importance attributed to each category.[21]

Voo et al. from the Belfer Center published the National Cyber Power Index (NCPI) in 2020. This index measures thirty countries' cyber capabilities in the context of seven broad categories called national objectives. The authors compiled and developed twenty-seven unique indicators to measure a state's cyber capabilities. The NCPI provides a comprehensive overall measurement of a country's aptitude as a cyber power with a combination of two standalone measures, the Cyber Capability Index (CCI) and the Cyber Intent Index (CII). The latter reflects the different prioritisation that some countries place on developing specific objectives, hence it can be considered equivalent to a weight.[22]

As Çifci (2022) also highlights the difficulties of measuring offensive cyber capabilities, one common limitation of these indices is the high level of secrecy on the related topics,[23] hence offensive cyber capabilities have also proven especially hard to measure objectively, given the lack of publicly available information. However, the continuing proliferation of offensive cyber capabilities also increases the visibility of an otherwise covert area of cybersecurity.

Additionally, the scope of these studies also seems to fall short, considering the unprecedented pace of proliferation. According to Marczak et al. (2018) from the Citizen Lab, while most cyber capability indices cover about thirty countries or less, the notorious Israeli cyber intelligence firm NSO Group provides services to operations in forty-five countries.[24] Furthermore, based on a document that surfaced during a lawsuit, another Israeli spyware firm, Candiru was negotiating deals with clients from over sixty countries.[25]

---

20 Demchak et al. 2015.
21 IISS 2021.
22 Voo et al. 2020.
23 Voo et al. 2020: 10.
24 Marczak et al. 2018.
25 Ziv 2020.

Indicators of offensive cyber capabilities

> "*Imagine that you are a chef. If you are a chef and you've got an empty kitchen, you will not be cooking anything. But if you are a chef and you've got some ingredients, then you can make some things. If I saw those ingredients, then I can kind of guess what you can make. But there comes a point where you don't know what is going to come out of the kitchen until you know who the chef is.*" – Julia Voo, 2020[26]

What indicators can we identify to assess offensive cyber capabilities without a clear definition to understand and scarce public information to measure? As explained by Liff (2012), although it may be simple to acquire a basic level of attack capability against computer networks, successfully attacking more secure systems or a more sophisticated adversary would require resources well beyond the means of conventionally weak actors.[27] At the same time, as highlighted by the Atlantic Council's Cyber Statecraft Initiative, the proliferation of offensive cyber capabilities shows that many governments are willing and able to pay the price to purchase the capabilities necessary for their various objectives. Even so, they cannot find the talent they need or cannot afford the expenses of in-house capability development lasting even decades. Meanwhile, Access-as-a-Service (AaaS) firms offer government-level capabilities at private sector speeds.[28] The continuous proliferation of cyber capabilities also increases the risk of incidents that draw public attention to otherwise concealed capabilities.

However, offensive cyber capabilities flow into all other aspects of society. Including, but not limited to, the digital economy as the Internet and technology transforms the way we do business, the national skill base needed for future economic development, or the university education required by today's information and knowledge-based society. Based on the International Institute for Strategic Studies (IISS), cyber capable countries also identify skills shortage as a significant risk, hence have embarked on upskilling and training initiatives. The cybersecurity skills shortage impacts the national labour markets worldwide, and the problem seems to persist, despite the proposed initiatives and launched actions.[29] It seems the skills shortage sets a common ground for understanding the importance of talent identification, development and management, which are all essential for both cyber capability development and cyber capacity building. Since zero-day vulnerabilities, crucial components of offensive cyber capabilities cannot be reused, the various actors in cyberspace need to develop their vulnerability research capabilities to identify new, previously unknown security flaws.

The question arises, why some states are incapable of producing the required cyber capabilities organically? It seems that research and education appear to be stronger in the liberal-democratic states, while the education systems of authoritarian countries

[26] AttackIQ 2020.
[27] Liff 2012: 401–428.
[28] DeSombre et al. 2021a.
[29] DeSombre et al. 2021a: 8.

remain underdeveloped. Similarly, Sanborn and Thyne (2013) highlight that authoritarian regimes typically underinvest in education, as education promotes democratisation. Hence, they misappropriate resources elsewhere.[30] Nevertheless, cyber-related research and education are difficult to implement without adequate public and higher education systems. The recently updated global inventory of commercial spyware initially compiled and released by Feldstein and Kot (2023) incorporates incidents from 2011 to 2023 and suggests a connection between the education system and the cyber power of a country, because "the data shows that autocratic regimes are far likelier to purchase commercial spyware or digital forensics than democracies".[31]

However, while defining and measuring cyber capabilities is difficult, assessing the educational capacities required for cyber talent identification, development and management may be a more straightforward approach. The different levels of the educational system, including elementary education, higher education and universities, are the core of cybersecurity competence. We can measure the availability of educational and training resources by indicators such as those described by Šendelj and Ognjanović (2015) and used by the Enhancement of Cyber Educational System of Montenegro (*ECESM*) project: organisational capacities; the number of courses, departments and study programs addressing cybersecurity issues; the number of organised training and workshops.[32] Aiming to attract students, the information behind these indicators is traditionally part of some publicly available curricula. The previously mentioned indicators can be further supplemented, for example, by the number of academic or professional security researchers, publicly disclosed security vulnerabilities, and online published technical analysis reports or custom-developed security tools.

One such resource is the Cybersecurity Higher Education Database (CyberHEAD), the largest validated cybersecurity higher education database in the European Union. Additionally, in their report about the European cybersecurity skills framework, Nurse et al. (2022) provide an overview of the current supply of advanced cybersecurity skills in Europe through an analysis of CyberHEAD. They collected the data via a questionnaire and supplemented the provided answers with publicly available information. The report includes the complete replies to questions that need to be answered by European academic institutions when listing their programs in CyberHEAD.[33]

Such raw data and information could serve as an appropriate basis for a more accurate assessment of cyber power, including offensive cyber capabilities. For example, Figure 1 below shows the distribution of cybersecurity education programs between European countries. Although these are only quantitative indicators, based on just the number of programs available, it seems that Spain (23), Italy (18), France (11) and Poland (11) are currently leading the way in cybersecurity upskilling. Their current educational advantage over other EU countries may be reflected in their future progress in offensive cyber capability development.

---

30 Sanborn–Thyne 2013: 773–797.
31 Feldstein–Kot 2023.
32 Šendelj–Ognjanović 2015.
33 Nurse et al. 2022.

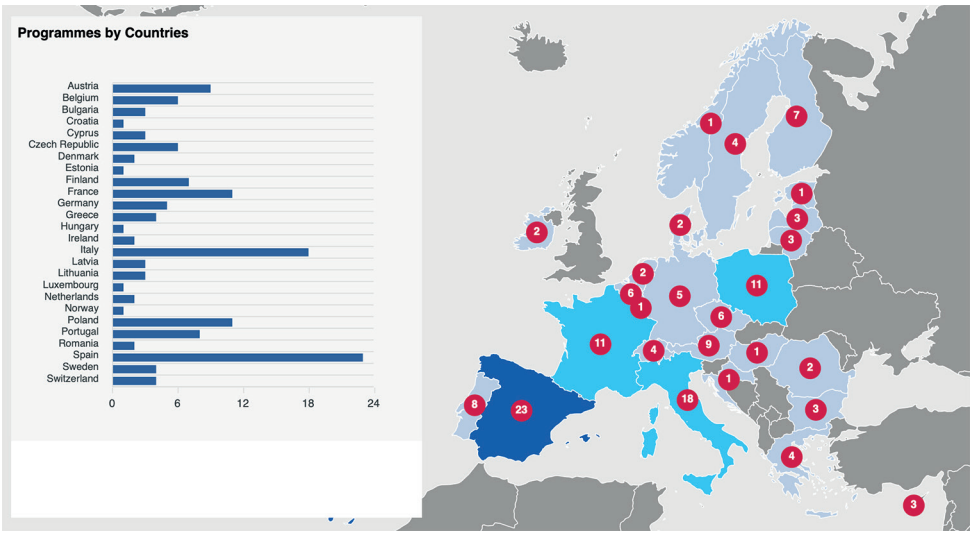

Figure 1: EU-wide distribution of cybersecurity programs registered in the CyberHEAD database in 2022

Source: ENISA 2023.

As also recognised by Xiangzhan et al. (2016), "competition between talented people […] is fundamental to international cyberspace security".[34] Given a supportive environment, cyber talents tend to stand out like islands in the sea through various individual or independent contributions during various hacker competitions. For example, the United States aims to reduce the skills shortage with the Cyber Challenge (USCC) program, launched to identify, attract and recruit the next generation of cybersecurity professionals. Young cybersecurity enthusiasts compete against each other online, and the top performers are invited for an in-person training program the following summer. Additionally, in 2019 former American president Donald J. Trump established the President's Cup Cybersecurity Competition (PCCC) for federal employees to identify cybersecurity talents inside the federal workforce.[35]

Hacking contests are also great places to scout for talented people. The number of participants and their results could be indicators of the offensive cyber capabilities of their indirectly represented nations. Mainly enterprises sponsor hacking competitions to publicise the security of a product and to use the security community to learn about new and innovative research techniques. They usually provide a commercially sold product and encourage the participants to find and exploit its vulnerabilities. Although Pwn2Own is the most famous hacking contest and offers the highest prizes in the world, Tianfu

[34] Xiangzhan et al. 2016: 49–52.
[35] Trump 2019.

Cup also became a notable contest in recent years after China banned its former winner security researchers from participating in Pwn2Own.[36]

Security researchers commonly share information on new vulnerabilities, methodologies, or techniques in the cybersecurity community. In the same way, it is also a common practice to share custom-developed software tools on collaborative coding platforms like GitHub or GitLab. Public technical analysis reports of notorious vulnerabilities, proof-of-concept exploits, or security software tools may draw attention to their author as a skilled professional or high-potential cybersecurity talent.

Hack the Box and TryHackMe are just a few of the well-known cybersecurity training and game platforms that are great for learning and testing a candidate's knowledge. Users in these Capture the Flag (CTF) games must find their way through vulnerable systems that are purposefully made insecure and collect flags to keep track of their progress. Users advance in the ranks by completing the challenges, and we can track their success on their public profiles, which makes their talent visible to everyone.

Vendors initiated bug bounty programs in the 1980s to allow security researchers to report vulnerabilities. In the ideal case, they incentivise hackers to do the right thing and report flaws to the developer. Current bug bounty programs are either managed internally by the vendor or by a third party like HackerOne or Bugcrowd. However, many programs offer public thanks and acknowledgment to the researchers, who can earn points for their reports and appear on public leader boards. As Miyashita and Eckert summarised in the year-end review of their 2022 bug bounty program, Microsoft awarded three hundred thirty-five security researchers across forty-six countries, supported by the below world map in Figure 2, showing the distribution of researchers based on their location. Based on the grey scale from one to seventy-seven, the order of countries with the most awarded researchers seems to be China, USA, India, the U.K., Germany and Eastern Europe also participated.[37]

Even though employers usually prohibit their staff from participating in hacking contests or bug bounty programs,[38] their employees still compete with others in the labour market, often with a publicly available resume highlighting key work achievements, skills and experience. Thereby the labour market can serve as indirect feedback to measure the overall performance of a cybersecurity educational system and the cyber capability of a country. The cybersecurity sector is always looking for skilled workers and will find them where the educational system can produce them.

Furthermore, the nature of the positions available in the labour market also plays a decisive role regarding cyber capabilities. Distinguishing between the added value of the various job roles is essential. For example, while an analyst has an important role in defence against cyberattacks, an exploit developer has a crucial impact on building offensive capabilities.

---

36 Blue 2018.
37 Miyashita–Eckert 2022.
38 Laszka et al. 2018: 138–159.

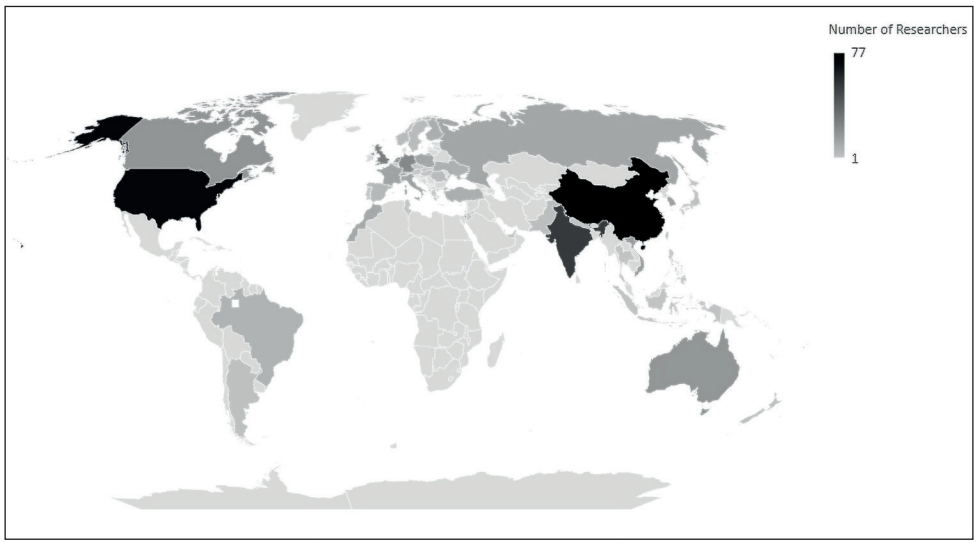

Figure 2: Worldwide distribution of security researchers awarded by Microsoft in 2022
Source: Miyashita–Eckert 2022.

The main advantage of the previously discussed indicators is that the necessary information is publicly accessible on the Internet. The data can be collected in an automated way, without questionnaires or interviews. The security community may ensure the authenticity and correctness of public information by early exposing false claims, especially regarding offensive security. After verification and validation, the data can be evaluated objectively.

Conclusion

Secrecy is the basis of offensive security. Assessing and measuring something that nation states want to keep secret and hidden is difficult, to say the least. Yet, if we take a holistic view of offensive security, we may find the signs by which otherwise hidden cyber capabilities can become investigable.

Offensive security requires human ingenuity and creativity, hence it is often more of an art than a science, and as such, it requires artists to do it. Allowing people to tackle challenges without constraints is the best way to bring out the best in them. Thereby, their shining talent will be something we can look for when assessing cyber capabilities. As young people hone their skills, they show their talent to the public. During this time, the secrecy that traditionally characterises the cybersecurity profession does not yet cover their activities. As a result, important information (blog posts, code repositories, competition results and resumes) is publicly available from this period, based on which cyber capabilities could be assessed and measured by a better approximation.

In this sense, the key to successful offensive cyber capability development is the size and quality of the available workforce, while the labour shortage affects all actors.

Whoever can first meet the challenge of the cybersecurity skills shortage, may win the cyber race. Though China has demonstrated its cyber power with its outstanding performance in the indicators mentioned earlier, due to its massive population scale and political establishment, the talent shortage may have a particularly negative impact on the country. According to a ministry report, China will have a more than three-million-person talent gap in cybersecurity by 2027, while its higher education institutions can only produce thirty thousand new professionals annually.[39]

Meanwhile, as Harvard University scholar Graham Allison and former Google CEO Eric Schmidt argued, though the United States faces the same problem, its immigration policy could offer a significant advantage in the race for talent.[40] Cybersecurity-specific agency actions, similar to those announced by the Biden–Harris Administration to attract international STEM talent,[41] would allow the U.S. to recruit and retain qualified foreign nationals who already possess the requisite skills, education and expertise, without investing the time and resources needed to train them. In contrast, China's great weakness is its inability to attract foreign talent, because it has limited itself to its own population, while the U.S. can recruit from all over the world.

References

Allison, Graham – Schmidt, Eric (2022): The US Needs a Million Talents Program to Retain Technology Leadership. Immigration is the United States' Secret Sauce – Including in Its Competition with China. *Foreign Policy*, 16 July 2022. Online: https://foreignpolicy.com/2022/07/16/immigration-us-technology-companies-work-visas-china-talent-competition-universities/

AttackIQ [@AttackIQ] (2020): Think Bad, Do Good: Julia Voo and the National Cyber Power Index. *YouTube*, 05 October 2020. Online: www.youtube.com/watch?v=OESUV5qRfdY

Billo, Charles – Chang, Welton (2004): Cyber Warfare – An Analysis of the Means and Motivations of Selected Nation States. *Institute for Security Technology Studies at Dartmouth College*, 01 November 2004. Online: www.researchgate.net/publication/230687826

Blue, Violet (2018): When China Hoards Its Hackers Everyone Loses. *Engadget*, 16 March 2018. Online: www.engadget.com/2018-03-16-chinese-hackers-pwn2own-no-go.html

Chawla, Gunjan – Srivastava, Vagisha (2020): What Are 'Offensive Cyber Capabilities'? *The CCG Blog*, 07 August 2020. Online: https://ccgnludelhi.wordpress.com/2020/08/07/what-are-offensive-cyber-capabilities/

Chivvis, Christopher S. – Dion-Schwarz, Cynthia: Why It's So Hard to Stop a Cyberattack – And Even Harder to Fight Back. *The RAND Blog*, 30 March 2017. Online: www.rand.org/blog/2017/03/why-its-so-hard-to-stop-a-cyberattack-and-even-harder.html

[39] Shen 2022.
[40] Allison–Schmidt 2022.
[41] The White House 2022.

Çıfcı, Hasan (2022): Comparison of National-Level Cybersecurity and Cyber Power Indices: A Conceptual Framework. *Research Square,* 17 October 2022. Online: https://doi.org/10.21203/rs.3.rs-2159915/v1

CSRC (2021): Vulnerability – Glossary. *NIST,* 2021. Online: https://csrc.nist.gov/glossary/term/vulnerability

Demchak, Chris – Kerben, Jason – McArdle, Jennifer – Spidalieri, Francesca (2015): Cyber Readiness Index 2.0. *Potomac Institute for Policy Studies,* November 2015. Online: https://potomacinstitute.org/images/CRIndex2.0.pdf

DeSombre, Winnona – Campobasso, Michele – Allodi, Luca – Shires, James – Work, JD – Morgus, Robert – O'Neill, Patrick Howell – Herr, Trey (2021a): A Primer on the Proliferation of Offensive Cyber Capabilities. *Atlantic Council,* 01 March 2021. Online: www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-primer-on-the-proliferation-of-offensive-cyber-capabilities/

DeSombre, Winnona – Shires, James – Work, JD – Morgus, Robert – O'Neill, Patrick Howell – Allodi, Luca – Herr, Trey (2021b): Countering Cyber Proliferation: Zeroing in on Access-as-a-Service. *Atlantic Council,* 01 March 2021. Online: www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/

Economist Intelligence Unit (2011): Cyber Power Index. Findings and Methodology. *Booz Allen Hamilton,* August 2011. Online: https://web.archive.org/web/20151017081309/www.boozallen.com/content/dam/boozallen/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf

ENISA (2023): *Cybersecurity Higher Education Database: Programmes Location.* Online: www.enisa.europa.eu/topics/education/cyberhead/#/statistics

Feldstein, Steven – Kot, Brian (2023): Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses. *Carnegie Endowment for International Peace,* 14 March 2023. Online: https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229

IISS (2021): Cyber Capabilities and National Power: A Net Assessment. *International Institute for Strategic Studies,* 28 June 2021. Online: www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

ITU (2021): Global Cybersecurity Index 2020. *International Telecommunication Union,* 29 June 2021. Online: www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Joint Chiefs of Staff (2018): *Joint Publication 3-12. Cyberspace Operations.* Online: https://irp.fas.org/doddir/dod/jp3_12.pdf

Kuehl, Daniel T. (2009): From Cyberspace to Cyberpower: Defining the Problem. In Kramer, Franklin D. – Starr, Stuart H. – Wentz, Larry K. (eds.): *Cyberpower and National Security.* University of Nebraska Press. 24–42. Online: https://doi.org/10.2307/j.ctt1djmhj1.7

Laszka, Aron – Zhao, Mingyi – Malbari, Akash – Grossklags, Jens (2018): The Rules of Engagement for Bug Bounty Programs. In Meiklejohn, Sarah – Sako, Kazue (eds.): *Financial Cryptography and Data Security.* Berlin–Heidelberg: Springer. 138–159. Online: https://doi.org/10.1007/978-3-662-58387-6_8

Liff, Adam P. (2012): Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, 35(3), 401–428. Online: https://doi.org/10.1080/01402390.2012.663252

Marczak, Bill – Scott-Railton, John – McKune, Sarah – Razzak, Bahr Abdul – Deibert, Ron (2018): Hide and seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. *Citizen Lab*, 18 September 2018. Online: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Minárik, Tomáš (2016): NATO Recognises Cyberspace as a "Domain of Operations" at Warsaw Summit. *NATO CCDCOE*, 21 July 2016. Online: https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/

Ministry of Defence (2018): *Joint Doctrine Note 1/18. Cyber and Electromagnetic Activities.* Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf

Miralis, Dennis (2019): Defining Offensive Cyber Capabilities. *NGM Lawyers*, 19 March 2019. Online: https://ngm.com.au/defining-offensive-cyber-capabilities/

Miyashita, Lynn – Eckert, Madeline (2022): Microsoft Bug Bounty Programs Year in Review: $13.7M in Rewards. *Microsoft Security Response Center*, 11 August 2022. Online: https://msrc.microsoft.com/blog/2022/08/microsoft-bug-bounty-programs-year-in-review-13-7-in-rewards/

Murphy, Ben – Creemers, Rogier – Kania, Elsa – Triolo, Paul – Neville, Kevin – Webster, Graham (2021): Xi Jinping: 'Strive to Become the World's Primary Center for Science and High Ground for Innovation'. *DigiChina at Stanford University*, 18 March 2021. Online: https://digichina.stanford.edu/work/xi-jinping-strive-to-become-the-worlds-primary-center-for-science-and-high-ground-for-innovation/

NATO Standardization Office (2020): *Allied Joint Publication-3.20. Allied Joint Doctrine for Cyberspace Operations.* Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

Nurse, Jason R. C. – Adamos, Konstantinos – Grammatopoulos, Athanasios – Di Franco, Fabio (2022): Addressing the EU Cybersecurity Skills Shortage and Gap through Higher Education. *Publications Office of the European Union*, 03 January 2022. Online: https://doi.org/10.2824/033355

Sanborn, Howard – Thyne, Clayton L. (2013): Learning Democracy: Education and the Fall of Authoritarian Regimes. *British Journal of Political Science*, 44(4), 773–797. Online: https://doi.org/10.1017/S0007123413000082

Sarri, Anna – Kyranoudi, Pinelopi – Thirriot, Aude – Charelli, Federico – Dominique, Yang (2020): National Capabilities Assessment Framework. *Publications Office of the European Union*, December 2020. Online: https://doi.org/10.2824/590072

Šendelj, Ramo – Ognjanović, Ivana (2015): Cyber Security Education in Montenegro: Current Trends, Challenges, and Open Perspectives. *7th Annual International Conference on Education and New Learning Technologies (EDULEARN15)*, 08 July 2015. Online: https://ecesm.net/sites/default/files/EDULEARN_Sendlej.Ognjanovic.pdf

Shen, Xinmei (2022): China's Demand for Cybersecurity Talent Will Exceed Supply by over 3 Million in Five Years, Says Education Ministry Report. *SCMP,* 08 September 2022. Online: www.scmp.com/tech/tech-trends/article/3191781/chinas-demand-cybersecurity-talent-will-exceed-supply-over-3

The White House (2022): Fact Sheet: Biden–Harris Administration Actions to Attract STEM Talent and Strengthen our Economy and Competitiveness. *The White House,* 21 January 2022. Online: www.whitehouse.gov/briefing-room/statements-releases/2022/01/21/fact-sheet-biden-harris-administration-actions-to-attract-stem-talent-and-strengthen-our-economy-and-competitiveness/

Trump, Donald J. (2019): America's Cybersecurity Workforce. *The White House,* 02 May 2019. Online: www.federalregister.gov/documents/2019/05/09/2019-09750/americas-cybersecurity-workforce

Uren, Tom – Hogeveen, Bart – Hanson, Fergus (2018): Defining Offensive Cyber Capabilities. *Australian Strategic Policy Institute, 0*4 July 2018. Online: www.aspi.org.au/report/defining-offensive-cyber-capabilities

Voo, Julia – Hemani, Irfan – Jones, Simon – DeSombre, Winnona – Cassidy, Dan – Schwarzenbach, Anina (2020): National Cyber Power Index 2020. *Belfer Center for Science and International Affairs,* September 2020. Online: www.belfercenter.org/publication/national-cyber-power-index-2020

Xiangzhan, Yu – Hongli, Zhang – Haining, Yu – Zhihong, Tian – Jianhong, Zhai – Zhuting, Pan (2016): Cyberspace Security Competition and Talent Management. *Strategic Study of Chinese Academy of Engineering,* 18(6), 49–52. Online: https://doi.org/10.15302/J-SSCAE-2016.06.010

Ziv, Amitai (2020): Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed. *Haaretz,* 07 September 2020. Online: www.haaretz.com/israel-news/tech-news/.premium-mobile-spytech-millions-in-gulf-deals-top-secret-israeli-cyberattack-firm-reve-1.9125915