Vladimir Tomašević
Faculty of Engineering Management
Email: vladimir.tomasevic@fim.rs

Luka Latinović
Faculty of Engineering Management
Email: luka.latinovic@fim.rs

DOI: https://doi.org/10.37458/ssj.5.3.11
Research Paper
Received: September 25
Accepted: November 9

6G AND 7G CELLULAR NETWORKS AS MERCENARY CYBER TERRORISM ENABLERS

Abstract: *As cyberspace became a new arena in geopolitics, state actors nurtured cyber mercenaries as a novel covert weapon. At the same time, technologies that required significant real-time information flows, such as unmanned aircraft systems, were available to a few entities that state actors could hardly overlook. With the advent of cellular network internet speeds, available to citizens, such as 5G and in the future 6G, and 7G, almost anyone with Internet access will be able to handle a tool that can be a dangerous weapon in the hands of mercenary cyber terrorists, not only in the lease of state but also non-state actors. This paper provides a correlation analysis between ICT price trends and the number of cyber-attacks. It was found that there is a strong positive correlation between the Internet access speed and the number of cyber-attacks, as well as that there is a strong positive correlation between the CPU computing power and the number of cyber-attacks. Although no causal relationship has been established, there is evidence to suggest that the number of cyber mercenary attacks will rise with the continuation of cellular network speed rise and ICT price decline.*

Keywords: *cyber operations, cyber mercenaries, cyber-attacks, global threat, computational speed, ICT price.*

INTRODUCTION

While offensive cyber operations have become an integral part of the foreign policies of many countries, cyber mercenaries, but also terrorist organizations, as well as companies started using the borderless cyber domain to achieve their strategic goals (Topor, 2020). As Maurer stated, *projecting coercive power through cyberspace is not only a state-centric affair but often a dynamic interplay between the state and actors detached from the state* (Maurer, 2018, p.17). Such modern-day mercenaries and privateers can impose significant harm undermining global security, stability, and human rights, and as Maurer (2018) argues, this raises important questions over control, authority, and the legitimacy of the use of cyber capabilities. These groups today possess great power, and not without a reason. It is energized by globalization and the democratization of technology (Widiatmaja & Rizqi, 2020). Computing and communication costs have fallen more than a thousandfold between the 1970s and the beginning of this century (Di Carlo, Savino & Politano, 2010; McCallum, 2021; Nielsen, 2021). As Joseph Nye, a prominent figure who proposed the theory of soft power stated, *when the price of any technology declines dramatically, the barriers to entry go down. Anybody can play the game* (Nye, 2012). Figure 1 shows a significant incline trend of cybercrime in the last decade, specifically, cyber-attacks with more than 1 million US dollars in reported losses. The question arises as to how correlated ICT technology development and cybercrime are. We argue that there is a strong positive correlation between the number of cyber-attacks and global average internet speed, while there is a positive correlation between number of cyber-attacks and average CPU computing power. Moreover, new generations of cellular networks, such as 6G, and 7G will provide global high-speed Internet coverage. This will further lower cyber terrorism entry barriers, allowing for the widespread use of various new technologies such as UAS, UAV, and others.

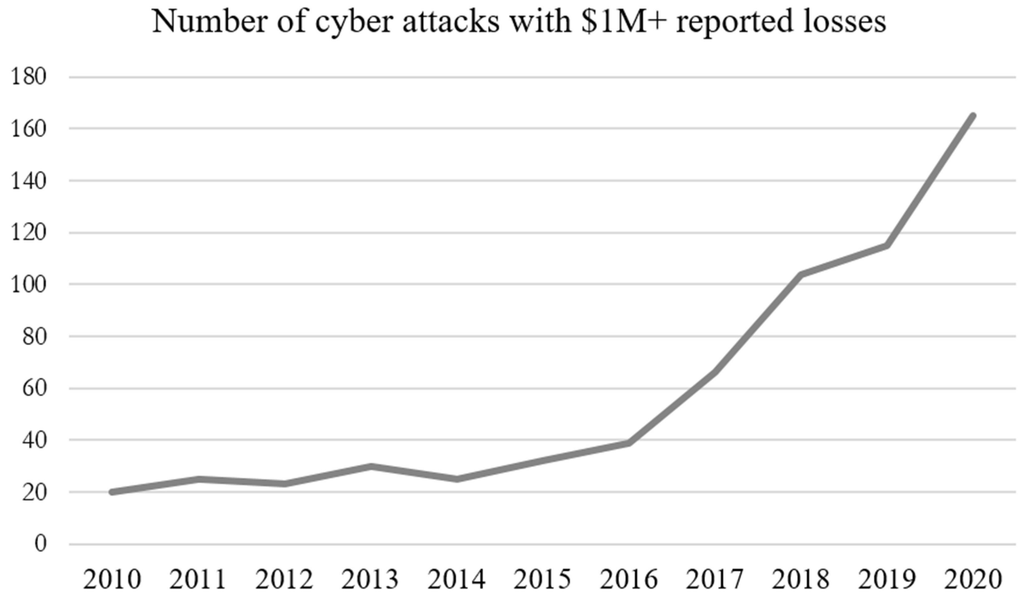


Figure 1: Number of cyber-attacks with more than 1 million US dollars reported losses.

METHODS

Based on the review of the relevant academic literature, the ICT evolution, and 6G and 7G cellular networks were analyzed in detail in heading 3 and heading 4, respectively. The analytic approach was conducted through the prism of cyber mercenary terrorism. In order to establish a relationship between the number of cyber-attacks and the global average Internet speed, as well as the number of cyber-attacks and the average CPU computing power, a correlative analysis was performed. Table 1 gives an overview of the three main data sets, collected over a ten-year period by the Security Institute of the Belgrade School of Engineering Management. Data was obtained by compiling a multitude of aggregated data from available international sources.

Table 1: Combined presentation of collected data on three key ICT trends - increase in the number of cyber-attacks, increase in computing power and internet speed.

	Set (i)	Set (ii)	Set (iii)
Year	Number of global cyber-attacks with	Estimated average global internet	Estimated average CPU power in GFLOPS

	$1M+ in reported losses	speed (Mbps)	
2010	20	1.9	15
2011	25	2.5	33
2012	23	3	44
2013	30	3.5	66
2014	25	4.7	83
2015	32	5.2	91
2016	39	6.5	121
2017	66	7.5	136
2018	104	11	169
2019	115	15	201
2020	165	21	245

The Pearson correlation coefficient (*r*) was chosen as a measure for bivariate correlation i.e., the ratio between the covariance of two variables and the product of their standard deviations. As with covariance itself, the measure can only reflect a linear correlation of variables and ignores many other types of relationships or correlations. The coefficient was calculated for the sets (i) and (ii), and the sets (i) and (iii) by the following equation:

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - x_{avg})(y_i - y_{avg})}{\sqrt{\sum_{i=1}^{n}(x_i - x_{avg})^2 \sum_{i=1}^{n}(y_i - y_{avg})^2}} \tag{1}$$

where:

r_{xy} - represents correlation coefficient;

n is sample size, which in this case is 11, one for each data sample from 2010 to 2020;

x_i, y_i are the individual data points with index i;

x_{avg}, y_{avg} are sample means, calculated for each dataset.

ICT EVOLUTION

Initially, the cost of computing was very high, making this technology reserved for state actors such as military or scientific entities. Computing machines were a large capital investment, and hard to obtain (Slominski, Muthusamy & Isahagian, 2019). This has radically changed due to the development of ICT, which took place simultaneously in two key areas, namely computing power and communication speed. As computing power increased in previous years, a significant decline trend in computing power price was recorded. At the same time, the average global internet connection speed has increased. Figure 1 gives a concise comparative view of computing power, disk drive, and wireless data transfer prices over the past decade. In addition to the appealing cost-effectiveness and high performance, GPUs also provide space, power consumption, and cooling requirement reduction in comparison to other parallel platforms. Another major breakthrough happened in the year 2012 when Raspberry Pi introduced the trend of microcomputers at a relatively low price (Johnston & Cox, 2017). This has enabled a significant proliferation of computers in the wider auditorium, even in developing countries (Basford et al., 2020). Although the development of computing power has caused a global decline in the price of personal computers, in addition to laptops, microcomputers have enabled covert installation and masking in various devices. However, despite the miniature size, these computers are quite potent and versatile (Chodorek, Chodorek & Wajda, 2019). Still, in order to come to full expression, computers need connection with other devices, and this gap has been filled by the development of wireless internet communication, which combined, has opened a whole new chapter on cyber-attacks.

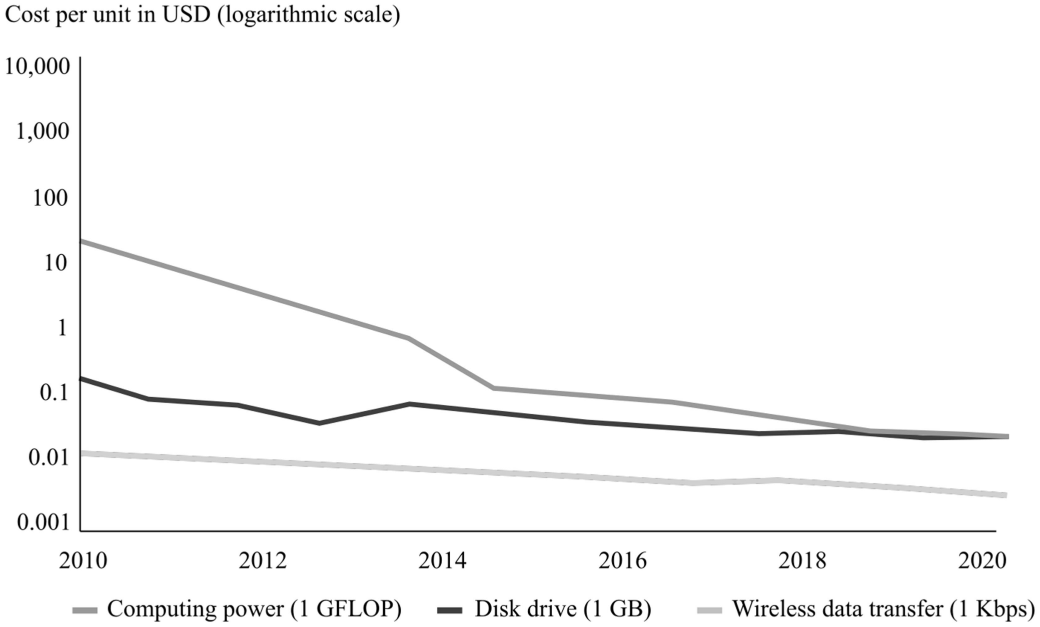
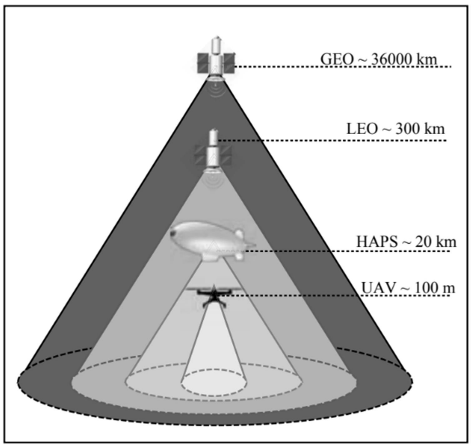


Figure 2: Continuous decline in prices of key ICT Data sources: (AI Impacts, 2021; McCallum, 2021; Nielsen, 2021)

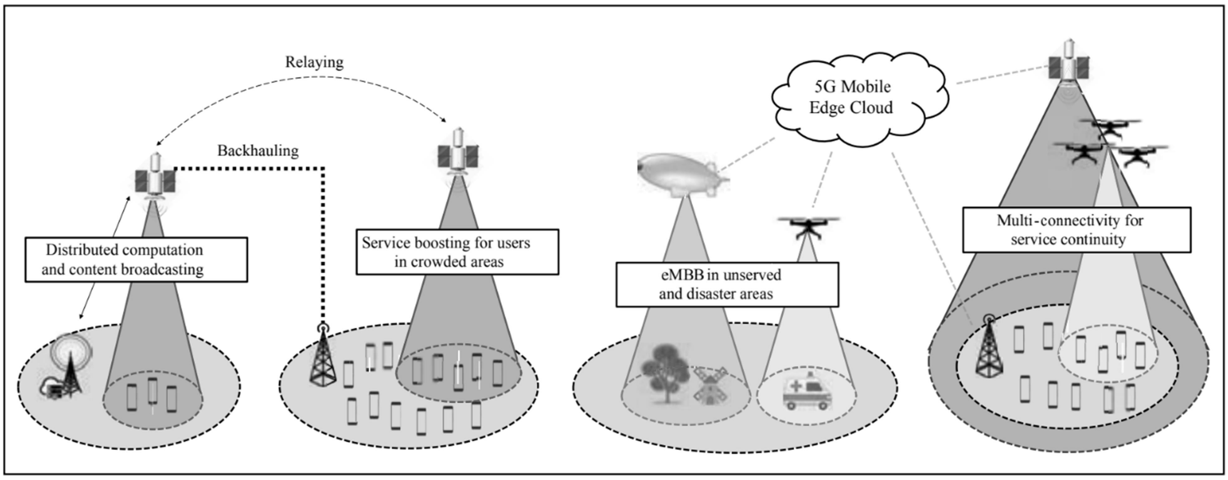
6G AND 7G CELLULAR NETWORKS

The past few decades have brought several cellular network generations, namely from 0G to 5G (Saad, Mehdi & Mingzhe, 2020). Each generation represented an incremental leap in connection speed from Kbps for starting generations, up to 100+ Mbps for 5G (Estifanos & Getamesay, 2021). In the relatively near future, further leaps are expected such as 6G and 7G. The sixth generation is aimed to be a ubiquitous ultra-broadband mobile network with ultra-high rate, ultra-high data density and ultra-low latency (Zong et al., 2019). This is supposed to combine the data interaction and computing collaboration of ubiquitous high-performance new generation of communication terminals (Zong et al., 2020). 6G architecture will shrink cells from small to “tiny cells”, but with denser deployment where mesh network and Device-to-Device (D2D) connectivity should become a norm (Saad et al., 2020; Bhat & Alqahtani, 2021; Hoschek, 2021). Performance bottlenecks of today’s common Internet of Things (IoT) devices such as latency, computing power and storage should be mitigated by increasing connections to other nodes (Sodhro et al., 2021). A reliable and low latency throughput is expected by calculations done by both, off-loading from the terminal to the IoT network, and off-loading from the network to the network, which should eventually become a commonplace feature of 6G (Hoschek, 2021).

Although this feature, As Saad et al. (2020) argue, indeed represents an increased threat surface allowing for a wider range of cyber-physical attacks on the network, at the same time it increases the network resilience (Porambage et al., 2021). Still, in order to achieve global connectivity, rural areas also have to be tackled. Densifying cellular sites involves large operational costs for network operators and requires high-capacity backhaul connections (Chen et al., 2020; Giordani & Zorzi, 2021). Network deployment in rural areas is further convoluted by the diversity of terrain configuration, and inevitably leads to an energy crunch with serious economic and environmental concerns (Giordani & Zorzi, 2021). To address these issues, 6G research is currently focused on the development of non-terrestrial networks (NTNs) to promote ubiquitous and high-capacity global connectivity (Mozaffari et al., 2019; Giordani & Zorzi, 2021). While previous wireless generation networks have been traditionally designed to provide connectivity for a quasi-bi-dimensional space, 6G envisions a three-dimensional (3D) heterogeneous architecture in which terrestrial infrastructures (Figure 3, b) are complemented by non-terrestrial stations (Figure 3, a) including Unmanned Aerial Vehicles (UAVs), High Altitude Platforms (HAPs), and satellites. Giordano and Zorzi, (2021) argue that *not only can these elements provide on-demand cost-effective coverage in crowded and unserved areas, but they can also guarantee trunking, backhauling, support for high-speed mobility, and high-throughput hybrid multiplay services*.



a)


Relaying
Backhauling
Distributed computation and content broadcasting
Service boosting for users in crowded areas
5G Mobile Edge Cloud
eMBB in unserved and disaster areas
Multi-connectivity for service continuity

b)

Figure 3. Non-terrestrial stations (a) and use cases enabled by the integration of terrestrial and non-terrestrial networks (b) (Giordano and Zorzi, 2021).

7G shell be another generation leap, from 6G to truly global coverage. It is aimed to be the most advanced generation in mobile communication but further research is required to tackle issues like using cell phones during moving conditions from one country to another country. This is due to the moving of satellites at a constant speed and in specific orbits, and unfit today's standards and protocols for cellular to the satellite systems and satellite-to-satellite communication systems (Estifanos & Getamesay, 2021). As these authors stated, *the dream of 7G can only be true when all standards and protocols are defined*. When 7G surpasses existing shortcomings, there should be no coverage and data capacity gaps. This has serious implications for cyber terrorism as it will be almost impossible to "turn off" the internet in a particular territory in case of need, due to the strong network resilience on account of D2D and P2P principles applications, and global internet providers.

RESULTS AND DISCUSSION

The Pearson correlation coefficient for the set (i), and set (ii), calculated by (1) amounted r=0.9831 (Figure 5). This is interpreted as a strong positive correlation between the two datasets.

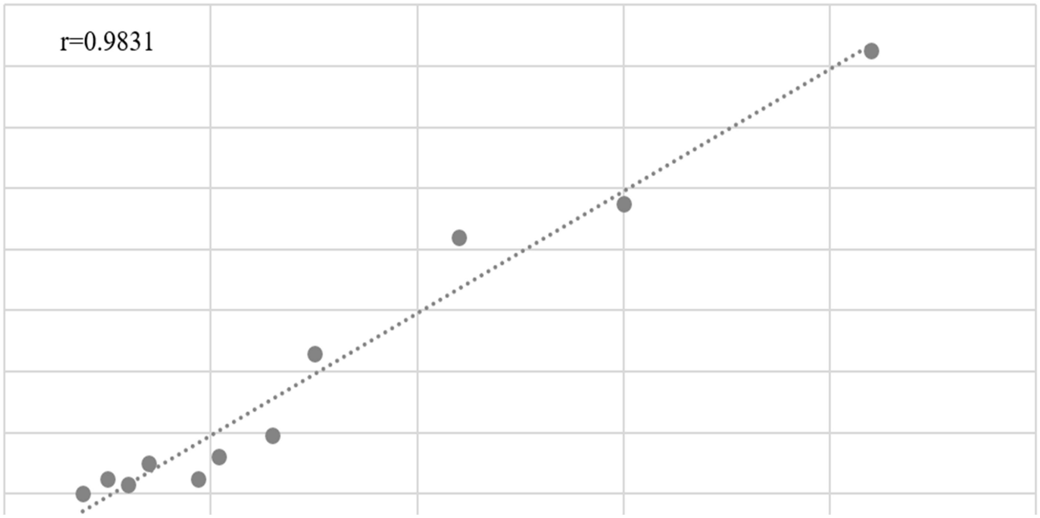


Figure 5: Pearson correlation chart for the set (i) (number of cyber-attacks) and set (ii) (average global internet speed)

The Pearson correlation coefficient for the set (i) and set (iii), calculated by (1) amounted r=0.9452 (Figure 6). This can also be interpreted as a strong positive correlation. Still, a rather lower correlation coefficient between sets (i) and (iii) compared to sets (i) and (ii) was somewhat expected. This can be attributed, at least partially, to the use of GPU technology as a complementary to the conventional CPUs. However, Internet speed and combined (CPU and GPU) computing power correlation analysis could not be performed as the data collected at the time, by the Security Institute of the Belgrade School of Engineering Management, related only to the average CPU computing power.

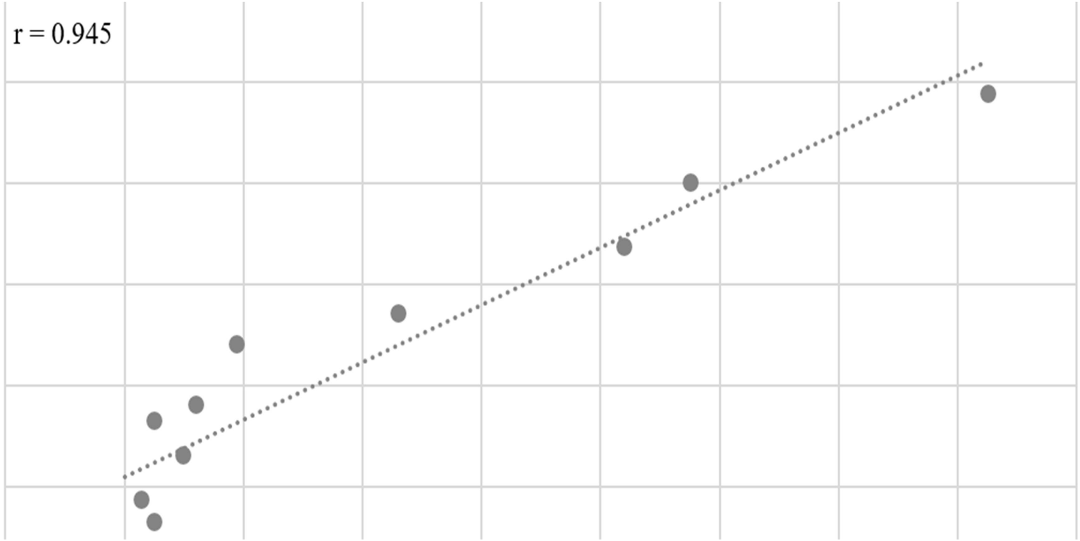


Figure 6: Pearson correlation chart for the set (i) (number of cyber-attacks) and set (iii) (computing power)

The correlation analysis results do not represent a radical, novel view of the facts, but rather mathematically prove the existence of underlying connections between them. Nevertheless, they provide enough evidence to support the assumption that an increasing number of cyber-attacks can be expected in the future. More importantly, the analytical approach of this paper to 6G and 7G technology has shown that their introduction will play a pivotal role in global security, as global high-bandwidth cellular networks will enable the real-time control of a variety of high-tech devices from remote locations. This is crucial because the immediate risk to the lives of mercenary terrorists will be reduced. This will inevitably lower the participating entry barriers allowing the reduction in their price. Finally, this will make their services available to a growing number of non-state actors such as various companies and individuals who will be able to hire them.

CONCLUSION

This paper established a strong correlation between the number of cyber-attacks and the global average Internet speed, as well as the number of cyber-attacks and the average CPU computing power. Moreover, the paper showed that 6G, and 7G cellular networks will introduce a radical change in the security paradigm regarding mercenary terrorism. These technologies will enable acts of terrorism in ways that have not been possible so far, in a significantly larger scope, posing a far larger global, as well as a local threat. Not only will states be able to choose from a large number of proxies, but non-state actors, such as companies and individuals, will also be influence competition or to settle accounts with opponents by hiring mercenary terrorists, if they have the financial means to do so. Therefore, we strongly appeal to all security structures to take the results of this work into account with due care. Timely creation of security strategies is imperative because this will be a burning issue in the relatively near future.

References

1. AI Impacts. Current FLOPS prices, (n.d). Accessed June 19, 2021. https://aiimpacts.org/current-flops-prices/

2. An, Xueli, Jianjun Wu, Wen Tong, Peiying Zhu, and Yan Chen. “6G Network Architecture Vision.” *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit),* 2021. https://doi.org/10.1109/eucnc/6gsummit51104.2021.9482439.

3. Basford, Philip J., Steven J. Johnston, Colin S. Perkins, Tony Garnock-Jones, Fung Po Tso, Dimitrios Pezaros, Robert D. Mullins, Eiko Yoneki, Jeremy Singer, and Simon J. Cox. “Performance Analysis of Single Board Computer Clusters.” Future Generation Computer Systems 102 (2020): 278–91. https://doi.org/10.1016/j.future.2019.07.040.

4. Bhat, Jagadeesha R., and Salman A. Alqahtani. “6G Ecosystem: Current Status and Future Perspective.” IEEE Access 9 (2021): 43134–67. https://doi.org/10.1109/access.2021.3054833.

5. Chen, Shanzhi, Shaohui Sun, Guixian Xu, Xin Su, and Yuemin Cai. “Beam-Space Multiplexing: Practice, Theory, and Trends, from 4G TD-LTE, 5G, to 6G and Beyond.” IEEE Wireless Communications 27, no. 2 (2020): 162–72. https://doi.org/10.1109/mwc.001.1900307.

6. Di Carlo, Stefano, Alessandro Savino, Gianfranco Michele Maria Politano, Alberto Scionti, and Alfredo Benso. “GPU Cards as a Low-Cost Solution for Efficient and Fast Classification of High Dimensional Gene Expression Datasets.” Control Engineering and Applied Informatics 12, no. 3 (2010): 34–40.

7. Estifanos Tilahun Mihret and Getamesay Haile. “Future Generations of Mobile Communication Networks.” American Journal of Computer Science and Information Technology 9, no. 2 (2021).

8. Giordani, Marco, and Michele Zorzi. “Non-Terrestrial Networks in the 6G Era: Challenges and Opportunities.” IEEE Network 35, no. 2 (2021): 244–51. https://doi.org/10.1109/mnet.011.2000493.

9. Hoschek, Miloslav. " Quantum Security and 6theseG Critical Infrastructure." *Serbian Journal of Engineering Management 6, no. 1* (2021): 1-8. https://doi.org/10.5937/SJEM2101001H.

10. Ilić, Damir, and Tomašević, Vladimir. "The impact of the Nagorno-Karabakh conflict in 2020 on the perception of combat drones." Serbian Journal of Engineering Management 6, no. 1 (2021): 9-21. https://doi.org/10.5937/SJEM2101009I.

11. Johnston, Steven, and Simon Cox. "The Raspberry Pi: A Technology Disrupter, and The Enabler of Dreams." *Electronics* 6, no. 3 (2017): 51. https://doi.org/10.3390/electronics6030051.

12. Manavski, Svetlin A, and Giorgio Valle. "Cuda Compatible GPU Cards as Efficient Hardware Accelerators for Smith-Waterman Sequence Alignment." *BMC Bioinformatics* 9, no. S2 (2008). https://doi.org/10.1186/1471-2105-9-s2-s10.

13. Maurer, Tim. Cyber Mercenaries: The State, Hackers, and Power. Cambridge, United Kingdom: Cambridge University Press, (2018).

14. McCallum, John C. "John C. McCallum Information Technology." Disk Drive prices 1955+, (2021). Accessed September 4, 2021. https://jcmit.net/diskprice.htm.

15. Mozaffari, Mohammad, Ali Taleb Zadeh Kasgari, Walid Saad, Mehdi Bennis, and Merouane Debbah. "Beyond 5G with Uavs: Foundations of a 3D Wireless Cellular Network." *IEEE Transactions on Wireless Communications* 18, no. 1 (2019): 357–72. https://doi.org/10.1109/twc.2018.2879940.

16. Nielsen, Jakob. "Nielsen Norman Group." Nielsen's Law of Internet Bandwidth, (2019). Accessed June 7, 2021. https://www.nngroup.com/articles/law-of-bandwidth/

17. Nye, Joseph S. Soft Power: The Means to Success in World Politics. Knowledge World, 2012.

18. Porambage, Pawani, Gurkan Gur, Diana Pamela Moya Osorio, Madhusanka Livanage, and Mika Ylianttila. "6G Security Challenges and Potential Solutions.*" 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit),* 2021. https://doi.org/10.1109/eucnc/6gsummit51104.2021.9482609.

19. Saad, Walid, Mehdi Bennis, and Mingzhe Chen. “A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems.” IEEE Network 34, no. 3 (2020): 134–42. https://doi.org/10.1109/mnet.001.1900287.

20. Slominski, Aleksander, Vinod Muthusamy, and Vatche Isahagian. “The Future of Computing Is Boring (and That Is Exciting!).” 2019 IEEE International Conference on Cloud Engineering (IC2E), 2019. https://doi.org/10.1109/ic2e.2019.00023.

21. Sodhro, Ali Hassan, Sandeep Pirbhulal, Zongwei Luo, Khan Muhammad, and Noman Zahid Zahid. “Toward 6G Architecture for Energy-Efficient Communication in IOT-Enabled Smart Automation Systems.” IEEE Internet of Things Journal 8, no. 7 (2021): 5141–48. https://doi.org/10.1109/jiot.2020.3024715.

22. Zong, Baiqing, Chen Fan, Xiyu Wang, Xiangyang Duan, Baojie Wang, and Jianwei Wang. “6G Technologies: Key Drivers, Core Requirements, System Architectures, and Enabling Technologies.” IEEE Vehicular Technology Magazine 14, no. 3 (2019): 18–27. https://doi.org/10.1109/mvt.2019.2921398.

23. Zong, Baiqing, Xiangyang Duan, Chen Fan, and Ke Guan. “6G Technologies - Opportunities and Challenges.*” 2020 IEEE International Conference on Integrated Circuits, Technologies and Applications (ICTA),* 2020. https://doi.org/10.1109/icta50426.2020.9332024.

24. Chodorek, Agnieszka, Robert R. Chodorek, and Krzysztof Wajda. “Media and Non-Media Webrtc Communication between a Terrestrial Station and a Drone: The Case of a Flying IOT System to Monitor Parking.” *2019 IEEE/ACM 23rd International Symposium on Distributed Simulation and Real Time Applications (DS-RT)*, 2019. https://doi.org/10.1109/ds-rt47707.2019.8958706.

25. Widiatmaja, Aji, and Fajria Hasta Rizqi. “The Rise of Non-State Actors in Globalization and Democratization Era: Terrorist Group Versus State Actors.” *Jurnal Sentris 2*, no. 2 (2020): 47–62. https://doi.org/10.26593/sentris.v2i2.4180.47-62.

26. Topor, Lev. “Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations.” The RUSI Journal 165, no. 1 (2020): 145–47. https://doi.org/10.1080/03071847.2020.1731150.