New Means of Communication — Sending Emotions through the Air?

NN

October 13, 2022

Seminar: Internet Economics, Talk No. 1

It is forecasted that 5G will trigger the early adoption of Augmented/Virtual reality (AR/VR). The spread of AR/VR applications will deplete the 5G spectrum, similar to how video-over-wireless saturated 4G networks, requiring a system capacity beyond 1 Tb/s rather than the 20 Gb/s targets specified for 5G. Typically AR/VR cannot be compressed to fulfill the latency requirements that enable real-time user engagement in the immersive environment (coding and decoding take time). The per-user data throughput must exceed a gigabit per second instead of the more relaxed 100 Mb/s 5G target [1].

It is therefore forecasted that techniques such as VR/AR will be essential for the presentation of enhanced communication needs of users. Furthermore, in 6G networks, the human urge to connect remotely with increased fidelity will stimulate significant communication issues. In the case enhanced communication techniques are used, the data rate requirements of a 3D holographic display, i.e., a raw hologram with no compression, colors, complete parallax, and 30 frames per second, would require 4.32 Tb/s. The latency needed will be sub-millisecond, and thousands of synchronized view angles, rather than the handful required for VR/AR, will be required [2]. Therefore, current 5G networks are still not designed to provide telepresence due to a relatively too low network capacity.

The crucial issue of future mobile networking is making innovative use of all network, service, and user data as well. Many novel services and network optimizations will be possible in the future based on collecting data and processing with suitable algorithms (machine learning, context awareness, and context filtering). This implies incorporating human sensory input (e.g., olfactory, tactile, and gustatory) [3], human biomedical information (e.g., heartbeat, respiration rate) [4] and users' emotions in future applications. The role of students is to explain the market potential behind new means of user-to-user communication stimulated by future 6G networks.

References

[1] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, “6g Wireless Networks: Vision, Requirements, Architecture, and Key Technologies,” IEEE Vehicular Technology Magazine, vol. 14, no. 3, pp. 28–41, 2019.

[2] M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, “Toward 6G Networks: Use Cases and Technologies,” IEEE Communications Magazine, vol. 58, no. 3, pp. 55–61, 2020.

[3] K. David and H. Berndt, “6g Vision and Requirements: Is There Any Need For Beyond 5G?” IEEE vehicular technology magazine, vol. 13, no. 3, pp. 72–80, 2018.

[4] S. Nayak and R. Patgiri, “6g communication technology: A Vision on Intelligent Healthcare,” in Health Informatics: A Computational Perspective in Healthcare. Springer, 2021, pp. 1–18.

Further reading and search for additional literature is required and recommended strongly!

An Economic Analysis of Ransomware Attacks: Should Companies Pay Attackers or Not?

NN

October 20, 2022

Seminar: Internet Economics, Talk No. 2

Ransomware is a type of malware in which an adversary attacks the availability and/or integrity of a victim's data, usually exploring encryption techniques [1]. The ransomware attack consists in an attacker asking victims to pay a ransom to recover their data and also avoid further leakages. Different approaches are recommended to prevent and/or recover from a ransomware attack, including effective backup strategies, staff security awareness training, up-to-date software, and monitoring tools [2].

Ransom payments are expected as a last attempt to recover from a ransomware attack. The ransomware market achieves records yearly, with multiple millions being paid to criminals yearly [3]. However, even after payments being made, there is no guarantee that the ransomware impacts will be solved, since many organizations never get access data to their data again after paying a ransom [4, 5]. Besides, these payments can have legal implications (e.g., international sanctions and measures to combat terrorism and its financing) [6]. Also, the ransom payments can have several implications on the reputation side and how a company is perceived by its customers.

The goal of this seminar is to understand the economics behind ransomware attacks and the companies' decisions to avoid or recover from them. For that, a literature review has to be initially conducted to map the different protection measures available and their costs. Next, the behaviors of both ransomware groups and companies have to be analyzed to understand when payments happen and how. Finally, economic analysis and discussions on ransom payments have to be provided. Thus, as an outcome of this seminar, an answer has to be provided to whether ransom payments can be considered a reasonable approach or not to reducing the economic impacts of ransomware attacks.

References

[1] A. Farion-Melnyk, V. Rozheliuk, T. Slipchenko, S. Banakh, M. Farion, O. Bilan: Ransomware Attacks: Risks, Protection and Prevention Measures; 11th International Conference on Advanced Computer Information Technologies (ACIT), Deggendorf, Germany, September 2021, pp. 473-478.

[2] I. A. Chesti, M. Humayun, N. U. Sama and N. Jhanjhi: Evolution, Mitigation, and Prevention of Ransomware; 2nd International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, October 2020, pp. 1-6.

[3] K. Oosthoek, J. Cable, G. Smaragdakis: A Tale of Two Markets: Investigating the Ransomware Payments Economy; arXiv:2205.05028, May 2022, Available at https://arxiv.org/abs/2205.05028

[4] D. winder: Ransomware Reality Shock: 92% Who Pay Don’t Get Their Data Back, May 2021, Available at https://www.forbes.com/sites/daveywinder/2021/05/02/ransomware-reality-shock-92-who-pay-dont-get-their-data-back/?sh=24095795e0c7

[5] SecureWorld: Ransomware: When Companies Pay Hackers, Do They Get Their Data Back?; February 2020, https://www.secureworld.io/industry-news/ransomware-when-companies-pay-hackers-do-they-get-their-data-back

[6] Y. Borboën, D. Bundi: Ransomware as a Business Model: Legal Aspects of Ransom Payment; PwC Switzerland, 2022, Available at https://www.pwc.ch/en/insights/cybersecurity/ransom-payment.html

Further reading and search for additional literature is required and recommended strongly!

The Internet of the Battlefield of Things (IoBT): Novelties and Economic Impact

NN

October 27, 2022

Seminar: Internet Economics, Talk No. 3

Today's battlefield and military operations are highly dependent on wireless communication technologies. Aircraft, warships, vehicles, weapons, and soldiers are equipped with connectivity capabilities to send and receive confidential information enabling successful offensive and defensive tactics. These deployments make up the so-called Internet of Battlefield Things (IoBT) [1], which combines the Internet of Things (IoT) characteristics with the requirements of military scenarios where properties such as security, privacy, and availability are even more critical than in civil scenarios. The dynamism of the IoBT, where troops, vehicles, and military equipment are constantly moving, requires wireless communications [2]. Therefore, the radio frequency (RF) spectrum should be managed securely and adequately to select unoccupied frequency bands, establish secure transmissions, intercept enemy messages, and decode valuable information. In the modern battlefield, cyberwar and cyberattacks are common hostile acts aiming to penetrate strategic targets such as enemy communications, area defense, or critical infrastructures [3]. In this context, IoBT devices are perfect targets due to their computational and storage constraints to maintain updated software and deploy cybersecurity mechanisms. The detection of the previous cyberattack families has been tackled separately by the literature. Most works analyze software operations to detect malware and exploit vulnerabilities in generic IoT devices deployed in military scenarios [4]. In summary, the main goal of this seminar consists of performing a technical and economical analysis of the novelties of the IoBT field in terms of i) devices, ii) communications, iii) cyberattacks, and iv) detection systems.

References

[1] S. Russell and T. Abdelzaher, “The internet of battlefield things: the next generation of command, control, communications and intelligence (c3i) decision-making,” in MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM). IEEE, 2018, pp. 737–742.

[2] D. Papakostas, T. Kasidakis, E. Fragkou, and D. Katsaros, “Backbones for internet of battlefield things,” in 2021 16th Annual Conference on Wireless On-demand Network Systems and Services Conference (WONS). IEEE, 2021, pp. 1–8.

[3] E. Izycki and E. W. Vianna, “Critical infrastructure: A battlefield for cyber warfare?” in ICCWS 2021 16th International Conference on Cyber Warfare and Security. Academic Conferences Limited, 2021, p. 45.

[4] P. Theron and A. Kott, “When autonomous intelligent goodware will fight autonomous intelligent malware: A possible future of cyber defense,” in MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM). IEEE, 2019, pp. 1–7.

Further reading and search for additional literature is required and recommended strongly!

Design Options for Decentralized Finance (DeFi) Protocols

NN

November 3, 2022

Seminar: Internet Economics, Talk No. 4

Decentralized finance (DeFi) was born from a hypothetical thought experiment of Vitalik Buterin, co-founder of the Ethereum blockchain, in 2016, when he proposed an idea of “on-chain decentralized exchanges”. This subsequently led to the creation of a decentralized financial system built on top of blockchains with Uniswap — a decentralized exchange/DEX —, the Maker Protocol — decentralized stablecoin —, and Compound — a decentralized lending at its foundations [1].

With the increasing Total Value Locked (TVL), DeFi protocols revealed to be susceptible to exploits, which are caused by design faults of the protocol itself or by the underlying blockchain [2, 4]. Furthermore, due to high transaction fees, DeFi protocols look for alternatives to Ethereum, especially in terms of other Layer-1 chains or Layer-2, and optimistic or zero-knowledge roll-ups [3].

This talk focuses on DeFi primities, blockchain scalability, and its related interoperability challenges. It investigates the architecture of DEXs, stablecoins, or other DeFi protocols and studies Layer-2 with respect to optimistic and zero-knowledge roll-ups.

References

[1] S. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, W. Knottenbelt: SoK: Decentralized Finance (DeFi), 2021. https://arxiv.org/abs/2101.08778

[2] L. Fang, B. Hor, E. Azm, K. Win Win: How to DeFi: Beginner/Advanced, CoinGecko, 2021

[3] A. Gangwal, H. Gangavalli, A. ThirupathiA Survey of Layer-Two Blockchain Protocols, 2022, https://arxiv.org/abs/2204.08032

[4] L. Heimbach, R. Wattenhofer: SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance, 2022. https://arxiv.org/abs/2203.11520

[5] Scaling | Ethereum.org Documentation. https://ethereum.org/en/developers/docs/scaling/, Last Access: September 17, 2022.

Further reading and search for additional literature is required and recommended strongly!

Cryptocurrency Scams: Overview and Classification

NN

November 10, 2022

Seminar: Internet Economics, Talk No. 5

Over the more than ten years of the mining of the first Bitcoin block, several Blockchain (BC) platforms have been developed and proposed. The BC concept brought benefits to several areas, such as supply chain tracking and money exchange [1]. However, as BCs often require an underlying cryptocurrency to provide incentives for participants to secure the network, the price of such currencies was prone to speculation, which led to an exponential increase in their value [2]. This increased value, allied to the pseudonym of BC transactions, caught the attention of cybercriminals that started to perform different attacks, such as phishing [3] and token scams [4]. One issue of these scams is that there is no clear taxonomy [5]; which hinders sharing data sets and the creation of novel detection approaches. Still, academia is engaged in providing scam detection and identification methods using different methods, such as clustering [6] and analyzing BC transactions [7]. Therefore, it can be seen that this is a novel and open-to investigation topic that addresses a significant problem within the BC area.

The goal of this seminar topic is to present a general overview of what cryptocurrency scams are, how they operate, their classification, types, and differences, and discuss these aspects. Further, the students can explore and survey different methods available in the literature to identify and detect such scams.

References

[1] E. J. Scheid, B. Rodrigues, C. Killer, M. Franco, S. Rafati, and B. Stiller, “Blockchains and Distributed Ledgers Uncovered: Clarifications, Achievements, and Open Issues,” Advancing Research in Information and Communication Technology, ser. IFIP AICT Festschrifts. Cham, Switzerland, Springer, August 2021, pp. 1–29.

[2] CoinMarketCap, “CoinMarketCap Market Capitalizations,” 2022, https://coinmarketcap.com/, last visit July 18, 2022.

[3] Y. Xia, J. Liu, and J. Wu, “Phishing Detection on Ethereum via Attributed Ego-Graph Embedding,” IEEE Transactions on Circuits and Systems II: Express Briefs, Vol. 69, No. 5, pp. 2538–2542, March 2022.

[4] . Xia, H. Wang, X. Luo, L. Wu, Y. Zhou, G. Bai, G. Xu, G. Huang, and X. Liu, “Don’t Fish in Troubled Waters! Characterizing Coronavirus-themed Cryptocurrency Scams,” APWG Symposium on Electronic Crime Research (eCrime 2020), Boston, MA, USA, November 2020, pp. 1–14.

[5] M. Bartoletti, S. Lande, A. Loddo, L. Pompianu, and S. Serusi, “Cryptocurrency Scams: Analysis and Perspectives,” IEEE Access, Vol. 9, pp. 148 353–148 373, October 2021

[6] R. Phillips and H. Wilder, “Tracing Cryptocurrency Scams: Clustering Replicated Advance-Fee and Phishing Websites,” IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2020), Toronto, ON, Canada, May 2020, pp. 1–8.

[7] J. Wu, Q. Yuan, D. Lin, W. You, W. Chen, C. Chen, and Z. Zheng, “Who Are the Phishers? Phishing Scam Detection on Ethereum via Network Embedding,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, Vol. 52, No. 2, pp. 1156–1166, September 2022.

Further reading and search for additional literature is required and recommended strongly!

On the Security of Processes: An Overview of Business Process Compromise (BPC) Attacks

NN

November 17, 2022

Seminar: Internet Economics, Talk No. 6

Infamous attack vectors such as DDoS attacks, botnets, cryptojackers, and ransomware have gained a lot of attention in the previous years. For example, the number of reported victims of Ransomware has doubled in 2021, making it one of the biggest cyber threats to organizations [1]. Many of these attacks are similar in that they first gain access to an information system and then exploit the victim financially. The latter part is done directly within the exploited information system. For example, the final goal of the ransomware is to render files within the file system useless to obtain a ransom at a later stage. Thus, these attacks deal damage quickly, however, they may also be detected in almost real-time due to their fast-acting operation [2].

The previously introduced attack vectors directly exploit the information systems involved in a business process. In contrast to traditional theft, this makes them harder to notice. Business Process Compromise (BPC) aims to make this exploitation even less transparent [3]. In BPC attacks, the first step is to gain internal information to understand the business process and the actors with their respective roles that are involved. Then, the attacker attempts to gain financial advantages by exploiting weaknesses in the business process [4]. For example, an attacker may learn that during the procurement process, a simple e-mail is sent to the accounting department which will then execute a transaction to settle the payments. An attacker could then rely on existing attack vectors, such as compromised electronic mail [5], to exploit the weakness of the business process by sending a forged e-mail holding a payment request.

This seminar topic aims to give an introduction to operational security concerns affecting processes. Specifically, commonly leveraged attack vectors used to carry out BPC attacks must be investigated. Finally, the impact of BPC attacks on businesses and potential recommendations as to how organizations can prevent or mitigate attacks has to be presented.

References

[1] PwC: “Cyber Threats 2021: A Year in Retrospect - PwC”; Available at https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-annex-download.pdf

[2] H. Oz, A. Aris, A. Levi, A. Uluagac: A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions; ACM Computing Surveys, February 2022

[3] S. Moodley, J. Hasewinkle: Hacking the Process - Business Process Compromise; Available at https://www.zyston.com/wp-content/uploads/Hacking-the-Process-Business-Process-Compromise.pdf

[4] mti: Security 101: Business Process Compromise; Available at https://mti.com/blog/2020/10/29/security-101-business-process-compromise/

[5] FBI: Business Email Compromise; Available at https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise

Further reading and search for additional literature is required and recommended strongly!

Sustainable Cybersecurity: Toward a Secure and Sustainable Cyber Ecosystem

NN

November 24, 2022

Seminar: Internet Economics, Talk No. 7

The development of innovative Information and Communication Technologies (ICT) has profoundly influenced the real world. As a result, the cyber world, the physical world, and human society have been densely interconnected and formed a new cyber-physical-social (CPS) ecosystem [1]. As a crucial concept for achieving coexistence between humans and nature, sustainable development is an essential guide for social and economic development [2]. In this highly complex CPS system, data plays a central role as the medium for communicating with the various entities in the system. Therefore, as a critical part of ICT, cybersecurity can contribute to realizing a sustainable CPS ecosystem[3]. For example, cybersecurity can ensure the integrity of environmental monitoring data and help researchers correctly understand the impact of climate change on the Earth's environment and ecosystem [4]. On the other hand, to protect the security of data and preserve users' privacy, cybersecurity methods consume many resources, from financial [5] to energy [6], and it is worth considering whether these investments are sustainable.

Sustainable cybersecurity aims to understand and rethink the role of cybersecurity technologies, mechanisms, and methods in environmental protection and sustainable development [2]. Accordingly, this seminar topic aims to present an overview of sustainable cybersecurity, how cybersecurity affects sustainable development, and what aspects a sustainable cybersecurity mechanism should consider. As an output of this seminar, students should summarize different qualitative and quantitative approaches to analyze the sustainability of cybersecurity through the currently available literature.

References

[1] D. F. Hsu, D. Marinucci, and J. M. Voas, “Cybersecurity: Toward a secure and Sustainable Cyber Ecosystem,” Computer, vol. 48, no. 4, pp. 12–14, 2015.

[2] S. Cassotta and R. Sidortsov, “Sustainable cybersecurity? rethinking approaches to protecting energy infrastructure in the European high north,” Energy Research & Social Science, vol. 51, pp. 129–133, 2019.

[3] A. Sulich, M. Rutkowska, A. Krawczyk-Jezierska, J. Jezierski, and T. Zema, "Cybersecurity and Sustainable Development," Procedia Computer Science, vol.192, pp. 20-28, 2021.

[4] J. Klein and K. Hossain, “Conceptualising human-centric cyber security in the Arctic in light of Digitalisation and climate change,” Arctic Review on Law and Politics, vol. 11, p. 1, 2020.

[5] H. Gutiérrez Ponce, J. Chamizo González, and M. Al-Mohareb, “Sustainable finance in cybersecurity investment for future profitability under uncertainty,” Journal of Sustainable Finance & Investment, pp. 1–20, 2021.

[6] M. Castaldo, A. Castiglione, B. Masucci, M. Nappi, and C. Pero, “Energy Awareness and secure communication protocols: The era of Green Cybersecurity,” Communications in Computer and Information Science, pp. 159–173, 2020.

Further reading and search for additional literature is required and recommended strongly!

An Overview into Pulse-Wave DDoS Attacks

NN

December 1, 2022

Seminar: Internet Economics, Talk No. 8

Pulse-wave DDoS attacks have lately been able to bring down vital network infrastructure while inflicting immense financial and reputational harm [1-4]. Pulse-wave attacks are gaining popularity among hackers because they allow attackers to target several victims in quick succession with brief, high-volume traffic bursts. The timesharing or multiplexing characteristic of such an attack, often alternating ”pulses” between two or more simultaneous targets, contributes to the popularity of such "bursting" DDoS attacks since it allows for more effective use of a Botnet. The design of a pulse-wave defense is complex [5]. As with traditional DDoS defenses, an ideal pulse-wave defense must first be general to recognize a diverse range of attack routes with varying granularity. This increases the detection difficulty by requiring fine-grained network monitoring to detect abrupt network changes. As such, the Internet economy of malicious activities follows the same maxims as any other: greatest efficiency and least cost. Pulse-wave DDoS attacks are extremely effective to offenders, in which their costs are comparable to other attacks while being able to increase the number of simultaneous targets.

The goal of this seminar is to expand the comprehension of the features and functioning of Pulse-wave DDoS attacks, presenting its definition and characteristics, and also the challenges towards detection and mitigation. The talk and report should also include an analysis of the economic impacts (e.g., higher cost-benefit for attackers and increased costs for detecting and defending such attacks). Students should present common types of botnets and their features, giving examples of attacks and how these can be mitigated.

References

[1] DDoS-Guard. Hidden Threat of Pulse Wave DDoS Attacks. URL: https://ddos-guard.net/en/info/blog-detail/hidden-threat-of-pulse-wave-ddos-attacks

[2] Sean Newman. Bursts, Waves and DDoS: What You Need to Know. URL: https://www.corero.com/blog/bursts-waves-and-ddos-what-you-need-to-know/

[3] I. V. Chugunkov, L. O. Fedorov, B. S. Achmiz and Z. R. Sayfullina, "Development of the algorithm for protection against DDoS-attacks of type pulse wave," 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018, pp. 292-294, doi: 10.1109/EIConRus.2018.8317090.

[4] Igal Zeifman. Attackers Use DDoS Pulses to Pin Down Multiple Targets, Send Shock Waves Through Hybrids. Imperva White-paper. URL: https://www.imperva.com/blog/pulse-wave-ddos-pins-down-multiple-targets/

[5] Albert Gran Alcoz, Martin Strohmeier, Vincent Lenders, and Laurent Vanbever. 2022. Aggregate-based congestion control for pulse-wave DDoS defense. In Proceedings of the ACM SIGCOMM 2022 Conference (SIGCOMM '22). Association for Computing Machinery, New York, NY, USA, 693–706. https://doi.org/10.1145/3544216.3544263

Further reading and search for additional literature is required and recommended strongly!

How does Public Trust Affect the Economic Value of IoT Products?

NN

December 8, 2022

Seminar: Internet Economics, Talk No. 9

In 2021 Apple introduced the AirTag [1], an object that can be attached to anything to keep track of its location, for example, keys, cats, or backpacks [2]. Since its release, the AirTag has resulted in numerous articles analyzing its functionality [3, 4] and revealing a more sinister misuse of the technology as spyware or stalkerware [5, 6, 7]. Among other concerns, especially the privacy users who do not participate in the Apple FindMy network is at risk, including Apple users who conciously do not wish to be tracked as well as users of other smartphone operating systems, since they are more easily tracked and not consistently notified. This poses the question of whether such easily misused and accessible tracking technology should be sold, especially since the safeguards put in place seem to be limited.

Hence, the students will investigate the Apple AirTag and other IoT products, which showcase a lack of privacy, to investigate how privacy affects public perception and trust [8, 9]. Overall, the students should gain an insight into the products and therefore their technology to judge for themselves if privacy is important and investigate how it affects market value.

References

[1] "AirTag - Technical Specifications", Support.apple.com, 2022. [Online]. Available: https://support.apple.com/kb/SP840?locale=en_US. [Accessed: 29- Aug- 2022].

[2] G. Fleishman, "13 AirTag Tracking Scenarios - TidBITS", TidBITS, 2022. [Online]. Available: https://tidbits.com/2021/05/15/13-airtag-tracking-scenarios/. [Accessed: 29- Aug- 2022].

[3] J. Purcher, "Two Massive Master Patents covering Apple AirTags has been Published illustrating many styles and Applications", Patently Apple, 2022. [Online]. Available: https://www.patentlyapple.com/patently-apple/2020/10/two-massive-master-patents-covering-apple-airtags-has-been-published-illustrating-many-styles-and-applications.html. [Accessed: 29- Aug- 2022].

[4] "Apple AirTag Teardown", TechInsights, 2022. [Online]. Available: https://www.techinsights.com/blog/apple-airtag-teardown. [Accessed: 29- Aug- 2022].

[5] G. Fowler, "Apple's AirTag trackers made it frighteningly easy to 'stalk' me in a test", The Washington Post, 2021. [Online]. Available: https://www.washingtonpost.com/technology/2021/05/05/apple-airtags-stalking/. [Accessed: 29- Aug- 2022].

[6] J. Clayton and J. Dyer, "Apple AirTags - 'A perfect tool for stalking'", BBC News, 2022. [Online]. Available: https://www.bbc.com/news/technology-60004257. [Accessed: 29- Aug- 2022].

[7] L. Bever, "She tracked her boyfriend using an AirTag — then killed him, police say", The Washington Post, 2022. [Online]. Available: https://www.washingtonpost.com/nation/2022/06/11/apple-airtag-murder-boyfriend-indianapolis-morris/. [Accessed: 29- Aug- 2022].

[8] C. Wilson, T. Hargreaves, and R. Hauxwell-Baldwin, 'Benefits and risks of smart home technologies', Energy Policy, vol. 103, pp. 72-83, 2017. https://doi.org/10.1016/j.enpol.2016.12.047

[9] J. Shin, Y. Park, and D. Lee, 'Who will be smart home users? An analysis of adoption and diffusion of smart homes', Technological Forecasting and Social Change, 2018.

Further reading and search for additional literature is required and recommended strongly!

Cyber War: Economic Impacts, Attribution, and Past Incidents

NN

December 15, 2022

Seminar: Internet Economics, Talk No. 10

Novel technologies have always revolutionized warfare throughout history, from gunpowder, aircraft and most recently to information technology[1]. Modern societies rely on a constant flow of information through computers and stable interconnectivity over the internet. The wide adoption of digitalization comes at the cost of exposing societies and armies to complex digital threats. Consequently, the virtual cyberspace has become the fifth domain of warfare besides land, sea, air and space [2]. Another facet of cyberwar is cyber-espionage, where giant amounts of data are exfiltrated from internal networks of companies and governments. A key challenge in cyberwar and cyber-espionage is attribution, i.e., determining who was behind an attack, because traces could be modified or removed completely. Only through thorough investigative work and analysis of traces and information attribution is possible, although can be asymmetrically high, or even simply impossible. Further, the deployment of cyber weapons in general is highly risky, as with nuclear weapons, the attacker can not be certain of the effects that it will have on another country. Overall, cyber espionage and cyberwar can have detrimental effects on societies and economies, examples are the attack on Solarwinds, causing an estimate of $100 billion in damages overall, or smaller attacks, such as the Distributed Denial-of-Service attacks on Estonia [3], where attribution to Russia was highly controversial. Other examples include Stuxnet[4], where highly sophisticated Advanced Persistent Threats (APT) were used to infiltrate and manpiluate nuclear enrichment facilities in Iran.

Thus, the goal of this talk is to explore the fundamental technological developments for managing conflict, waging war and creating dysfunction in modern societies, while analyzing the economic impact and also objectively discussing attribution of cyber attacks with examples of past incidents.

References

[1] E. Halpin, P. Trevorrow, D. Wright: "Cyberwar, Netwar and the Revolution in Military Affairs", 2006, Palgrave McMillan, London, ISBN 978-1-349-54123-2..

[2] E. Van Wie Davis, Shadow Warfare: Cyberwar Policy in the United States, Russia, and China. Rowman & Littlefield Publishing Group, Incorporated, 2021

[3] M. Lesk: "The New Front Line: Estonia under Cyberassault," in IEEE Security & Privacy, Vol. 5, No. 4, pp. 76-79, July-Aug. 2007, DOI: 10.1109/MSP.2007.98

[4] James P. Farwell & Rafal Rohozinski: "Stuxnet and the Future of Cyber War", 2011, Survival - Global Politics and Strategy, pp. 23-40, DOI: 10.1080/00396338.2011.555586

Further reading and search for additional literature is required and recommended strongly!