Security and Rights in CyberSpace: Cyber Social Security

Valentina Antoniol[1,†], Vita Santa Barletta[1,*,†], Fabiana Battista[1,†], Paolo Buono[1,†], Danilo Caivano[1,†], Giuseppe Campesi[1,†], Giuseppe Cascione[1,†], Antonietta Curci[1,†], Marco de Gemmis[1,†], Vincenzo Gattulli[1,†], Rosa Scardigno[1,†], Annita Larissa Sciacovelli[1,†], Patrizia Sorianello[1,†] and Vincenzo Tamburrano[1,†]

[1]*Università degli studi di Bari Aldo Moro, Piazza Umberto I, 70121 Bari, Apulia, Italy*

Abstract

The convergence of data from social media, mobile devices, and urban sensors is enabling deep analyses of human behavior, fostering the development of innovative services through the Social Sensing paradigm, where users act as human sensors. This vision, enhanced by Natural Language Processing (NLP) techniques applied to textual data from platforms such as X and Facebook, is crucial for extracting meaningful insights from the digital environment. In parallel, the rising interconnection between cyberspace and real-world events necessitates robust cognitive, methodological, and cyber-physical infrastructures to support civil society resilience. This article presents a logical architecture along two dimensions: Horizontal and Vertical. The Horizontal dimension is characterized by the five domains of Cyber Social Security (i.e., Cyber Intimate Partner Violence, Cyber Gender-based Violence and Stereotype, Cyber Hate Speech and Falsehoods, Urban Mapping & Privacy, Ethical and Political Risks). The Vertical dimension identifies the three security operating units: Detection, Response, and Prevention. Leveraging the new knowledge gained in each domain, the intersection between these two dimensions allows for the redefinition of detection rules in Cyber Social Security, formulating new response plans and preventing both known and emerging security threats.

Keywords

CSS, Cyber Social Security, Cybersecurity, Generative AI

1. Introduction

Cyber Social Security (CSS) emerges as an indispensable glue for facilitating a positive transposition of cyberspace-related events into the real (political-social-cultural) world [1]. Gleichzeitig, it serves as a protective barrier, preventing the potential transference of risks from the virtual realm to the physical world [2]. The application of tools and the use of diversified means of collecting, analyzing, and cataloguing data enable both the understanding of complex phenomena, based on human behavior, and the development of services that function as indispensable resources for defining a real improvement in individual and collective well-being.

The collection and analysis of data, related to the proper interpretation of human and social behavior (both in micro-physical and macro-physical terms), constitute one of the central nodes of the entire CSS research work[1]. Only through the collection and analysis of data can the relationship between cyberspace and the real world be fruitfully adjusted through the construction of appropriate predictive and intervention models.

So, the goal of this research is to address these issues through the proposition of multidisciplinary methods, techniques and tools (IT, psychological, economic, legal, engineering, related to social sciences)

COL-SAI 2025: Workshop on COllaboration and Learning through Symbiotic Artificial Intelligence, in conjunction with the 16th Biannual Conference of the Italian SIGCHI Chapter (CHItaly 2025), October 6-10 2025, Salerno, Italy (2025

*Corresponding author.

†These authors contributed equally.

valentina.antoniol@uniba.it (V. Antoniol); vita.barletta@uniba.it (V. S. Barletta); fabiana.battista@uniba.it (F. Battista); paolo.buono@uniba.it (P. Buono); danilo.caivano@uniba.it (D. Caivano); giuseppe.campesi@uniba.it (G. Campesi); giuseppe.cascione@uniba.it (G. Cascione); antonietta.curci@uniba.it (A. Curci); marco.degemmis@uniba.it (M. d. Gemmis); vincenzo.gattulli@uniba.it (V. Gattulli); rosa.scardigno@uniba.it (R. Scardigno); annitalarissa.sciacovelli@uniba.it (A. L. Sciacovelli); patrizia.sorianello@uniba.it (P. Sorianello); vincenzo.tamburrano@uniba.it (V. Tamburrano)

0000-0002-0163-6786 (V. S. Barletta)

[1]https://serics.eu/services/spoke-3-attacchi-difese

capable of operating a Cyber-Social risk management in civil society. To this end, it is necessary to reinterpret the functions of Cyber Security in Cyber Social contexts: Detection, Response, and Prevention.

Therefore, in order to design a framework that integrates the different perspectives of Cyber Social Security, the following research goals were identified:

- *Innovations for Cyber Social Detection*
- *Innovations for Cyber Social Response*
- *Innovations for Cyber Social Prevention*

2. Challenges in Cyber Social Security

Cyber Social Security (CSS) is a complex and multi-disciplinary field that encompasses the study of cyber-mediated changes in human behavior and activity, as well as the development of cyber infrastructure to protect society from cyber threats [3, 1]. The rapid growth of social media and the sharing of information through digital channels has created new vulnerabilities and threats, necessitating the need for robust security measures [4]. Therefore, CSS faces numerous challenges that stem from the ever-evolving landscape of cyber threats and attacks [5]. These challenges include the detection of malware, authentication, steganalysis, and the increase in the extent and nature of cyber-crimes [6, 7]. Additionally, the innovations in information technology, while creating new economic and social opportunities, pose challenges to security and expectations of privacy in smart cities [8, 9]. Furthermore, the lack of a universally agreed-upon definition of key terminology in the cybersecurity domain poses a major challenge to international treaties and arms control agreements [10]. So, the politics of cybersecurity are influenced by conceptions of time and temporality, shaping it as a political practice.

The challenges also extend to the need for more focused research to understand how social capital affects knowledge creation in the context of organizational cyber-security risk-related activities [11]. Moreover, the challenges of cybersecurity are compounded by the misuse of technical infrastructure for cyber deviant and criminal behavior, including the spreading of extremist and terrorism-related material, online fraud, and cybersecurity attacks [12]. These challenges necessitate a comprehensive approach to cyber social security, including the development of effective cyber security strategies, the implementation of cyber security operations centers, and the pursuit of legitimate security and the common good in contemporary conflict scenarios [13, 14, 15]. Additionally, the significance of process comprehension for conducting targeted attacks and the application of artificial intelligence to cybersecurity are crucial in addressing these challenges [16, 17]. Furthermore, the need for liability-based trust frameworks and the influence of cyber insurance services on cybersecurity are important considerations in mitigating these challenges [18].

The challenges in cyber social security are multifaceted and require a holistic approach that encompasses technological, social, and legal dimensions to effectively address the evolving cyber threats and attacks.

3. CSS Architecture

Social cybersecurity is an emerging scientific area focused on technology and social context [1]. In the realm of cybersecurity, significant attention has been directed towards assaults targeting and exploiting the cyber infrastructure to disrupt technology, pilfer or obliterate information, and misappropriate funds or identities [19]. Conversely, within the domain of social cybersecurity, the focus shifts to the influence or manipulation of individuals, groups, or communities, thereby shaping their behaviors with a particular emphasis on socio-political and cultural repercussions.

So, in a scenario where cyberspace events impact the real world and influence the political, social, and cultural spheres, it is essential to have the cognitive, methodological superstructures as well as the cyber-physical infrastructures necessary to guarantee the resilience of civil society.

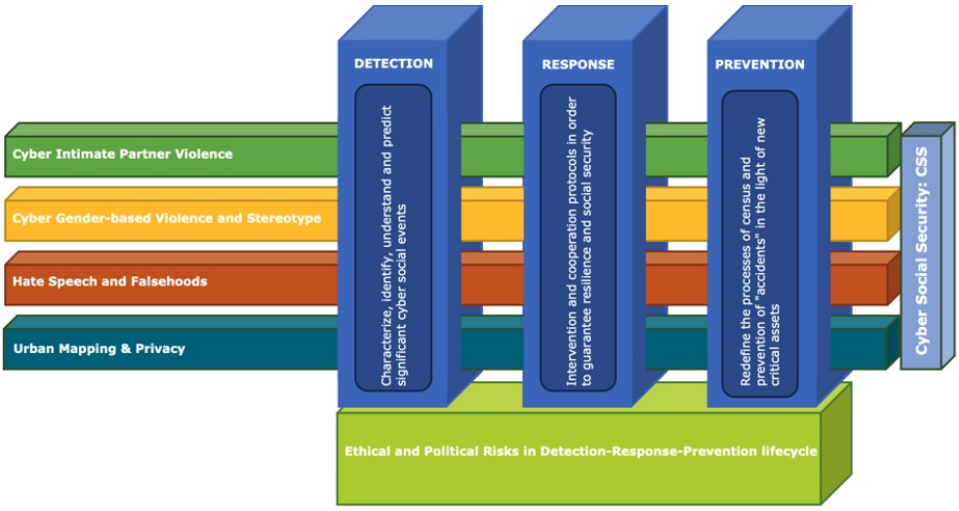

Figure 1: CSS Architecture

The reinterpretation of cybersecurity functions in the social context will take place along two dimensions: horizontal and vertical. The horizontal dimension (HD) currently involves the identification of 4 +1 key domains:

- **HD.1**: *Cyber Intimate Partner Violence (IPV).* IPV encompasses a range of abusive and aggressive behaviors perpetrated by one individual against their intimate partner [20, 21, 22]. These behaviors manifest in distinct patterns, including physical violence, sexual violence, stalking, and psychological aggression [21]. Physical violence involves the deliberate use of force with the aim of causing harm and physical injuries. Sexual violence pertains to sexual advances or actions carried out without the consent of the victim. Stalking entails repetitive and unwanted attention and communication that induces fear or apprehension regarding personal safety, whether the victim's safety or that of another person. Lastly, psychological aggression involves communication intended to adversely affect the mental and emotional well-being of the partner, ultimately establishing control over them. Studies have shown that the duration and severity of these behaviors can vary significantly, such that they can be isolated incidents or persist over multiple years [22].
  Therefore, considering the state of the art on Cyber-Intimate Partner Violence, to delineate prevention controls and functions for managing CSS, the following macro-categories of C-IPV will be analyzed:
  - Cyber Psychological Aggression
  - Cyber Sexual Aggression
  - Cyber Stalking Behaviors
- **HD.2**: *Cyber Gender-based Violence and Stereotype.* Among the several ways the performative strength of language and discourses can manifest, a deep impact concerns their capability to both reflect and influence societies, specifically referring to their perceptions and representations of social phenomena and groups, as in the gender case. Despite the constant efforts to promote bias-free and non-sexist writing to empower fairness movements, the perception of gender roles still represents a critical issue, hence the presence of biased socio-cultural expectations until these days [23]. As a heavily widespread type of unfair social attitudes and behaviors, gender inequality represents a multifaceted phenomenon implying a considerable loss of human potential: it can lead to perpetuating a culture of violence, higher gender wage gaps, and fail to represent women in higher and leadership positions [24].
- **HD.3**: *Cyber Hate Speech and Falsehoods.* The goal is to identify the contexts that facilitate verbal violence and deception, both in everyday conversation and in online language. The subject has a

distinctive character, not only within national borders, but also at the international level. Previous research has primarily focused on the lexical components of deceit, along with the emotional and psychological factors. Deception and hate speech pose potential risks for society and can result in numerous negative psychological and social consequences, whether directly or indirectly caused. When examining the linguistic aspects surrounding the topic, it is apparent that deception and hate speech share several characteristics. They carry negative connotations and are intentional. Additionally, the most vulnerable individuals, such as children, the elderly, women, and the disabled, are often the preferred targets of deceitful behaviour and hate speech. These behaviours are not novel as they have been linked to human nature and documented since ancient times. Nonetheless, in recent years, due to the ever-expanding prevalence of social networks and media, these phenomena have alarmingly multiplied. Consequently, a new linguistic phenomenon, fake news, has emerged along with a new social group, known as haters. In-depth analysis is required for lying and hate speech in both spoken and written language.

- **HD.4**: *Urban Mapping & Privacy.* The analysis in the urban context will be performed according to a vision based on two layers, which identify the initial taxonomy for further exploitation. The first layer is referred to as the real/physical layer in which we move and act every day: it involves indoor and outdoor environments, urban spaces, motion solutions, streets, public and private environments, other individuals, etc.. The second layer is referred to as the digital environment, which includes the set of social networks, messaging apps, traditional web sites, etc.. It is clear that the two layers are not independent of each other: they have strong interconnections and several connection points.
- **HD.5**: *Ethical and Political Risks.* In Cyber Social Security, this dimension revolves around the tension between protecting privacy and the risks of social control through data practices. While these systems safeguard against cyber threats, fake news, and attacks on critical infrastructure, the processes of data mining and analysis pose risks of privacy violations and pervasive social surveillance. This duality reflects two sides of the same coin: the protection of individuals versus the potential for opaque tracking, manipulation, discrimination, and human rights infringements. Key ethical concerns include lack of transparency about data collection, usage, and control; risks of influencing public opinion and behavior; and unequal access to services based on politically or socially identified groups. The political dimension highlights the transformation of personal data into economic value, raising issues of fairness and justice in how individuals' data is used, with a call to recognize data contributors as collaborators and workers deserving rights and benefits. Mitigating these risks requires informed consent, anonymization, data minimization, and adherence to principles of fairness, equality, and respect for human dignity. Ultimately, the sociopolitical challenge is to design Cyber Social Security technologies that empower communities and enhance collective welfare, rather than reinforce exploitative, opaque control systems.

The first 4 domains concur to realize the context of Cyber Social Security where the goal is not only to identify violence in its domain of appartence (psychological, linguistic, social, ethical, geopolitical, cyber, technological) but to identify new methods and techniques to redefine and/or identify new factors for defining such violence through the knowledge and lessons learned from each domain. Instead, for the fifth domain, ethical and political risks will be analyzed for the management of the social context and that underlie the Detection-Response-Prevention life cycle.

The vertical dimension (VD) is identified by the three security operating units:

- **HV.1**: Detection;
- **HV.2**: Response;
- **HV.3**: Prevention.

These models can be mapped to three organizational structures to ensure the security of people and information, together with the cyber social security controls contained therein:

1. *Security Operation Center in CSS (**Detection**)*: characterize, identify, understand and predict significant cyber-mediated events and changes in human, social, cultural and political behavior as

well as the methods for monitoring and protecting "social" end-points, thus being able to operate with devices (IT and IoT) and diversified information sources (OSINT/CLOSINT), taking into account the national and international legal framework (GDPR, NIS, CyberSecurity Act).

2. *Security Incident Response Team in CSS (**Response**)*: defining intervention and cooperation protocols between the main players in civil society in order to guarantee resilience and social security, including through homeland security technologies and the fight against cyber terrorism and cybercrime. The review of the Detection-Response-Prevention cycle will also clarify the limits within which it is possible to find and manage information while protecting the citizens' right to privacy and the security of civil society.
3. *Security Support Unit in CSS (**Prevention**)*: redefine the processes of census and prevention of "accidents" in the light of new critical assets (individuals, groups, communities, software applications and infrastructures for the public service, etc.), including elements of physical, organizational and applicative security as well as socio-political, economic, psychological and legal context.

Figure 1 shows the identified logical architecture. The result of the interaction between security functions and social dimensions helps to redefine detection rules in CSS, formulate new response plans, and prevent both known and unknown attacks and cyber social incidents based on the new knowledge gained in each domain. In particular, the intersection of the three security functions with a specific social dimension enables the redefinition of the Detection-Response-Prevention lifecycle for each domain (Output of the Horizontal dimension). At the same time, the intersection of the five social dimensions with a specific security function allows the redefinition of existing activities or the creation of new processes based on these insights. As a result, security operational units derived from these activities can be extended (Output of the Vertical dimension). The definition of the three operational units along the Vertical dimension allow to manage the impact on *Cyber Social Security*.

4. Artificial Intelligence in Cyber Social Security

The integration of Artificial Intelligence (AI) into Cyber Social Security represents a transformative opportunity to enhance the effectiveness and scalability of detection, response, and prevention mechanisms across socio-technical domains. Given the complexity and multidimensionality of CSS—spanning psychological, technological, legal, and socio-political layers—AI provides powerful capabilities to process, analyze, and learn from heterogeneous data sources, enabling real-time insights and adaptive intervention strategies. Therefore, AI can act as a cross-cutting enabler across both the Horizontal Dimension and the Vertical Dimension (Detection, Response, Prevention). By leveraging machine learning, natural language processing, and social network analysis, AI systems contribute to redefining detection rules, formulating targeted responses, and anticipating emerging threats that stem from cyber-mediated behaviors.

A concrete application of AI within CSS can be illustrated through the domain of Cyber Hate Speech and Falsehoods, one of the key areas identified in the CSS Horizontal Dimension. This domain deals with the identification of harmful, deceptive, and emotionally manipulative language disseminated via digital platforms, often targeting vulnerable social groups and threatening public cohesion.

- *Detection (HV1).* AI-powered Natural Language Processing (NLP) tools are deployed to analyze real-time streams of content from platforms like X, YouTube, or Telegram. Transformer-based models (e.g., BERT, RoBERTa) trained on annotated corpora can automatically flag content containing hate speech, misinformation, or incitement to violence. These tools can identify both explicit slurs and implicit or coded language, considering linguistic, cultural, and emotional context.
- *Response (HV2).* Once identified, the incidents are automatically categorized and routed to appropriate authorities. AI systems support incident prioritization based on severity, potential virality, and impacted communities. Visual dashboards and narrative explanations generated

through explainable AI (XAI) help stakeholders (e.g., social platforms, policy-makers, educators) understand the nature and trajectory of the threat.

- *Prevention (HV3).* Longitudinal AI models are used to monitor trends, simulate propagation patterns, and predict high-risk periods (e.g., elections, social unrest). The insights derived support the co-creation of digital awareness campaigns, content moderation policies, and community-level interventions to increase resilience and counter hate normalization online.

In addition, Generative AI has emerged as a transformative technology with significant implications across multiple domains. The potential of generative AI in CSS context lies in its ability to synthesize, analyze, and generate complex content that can enhance detection, prevention, and response strategies against evolving cyber-social threats.

Generative AI models, such as large language models (LLMs) and generative adversarial networks (GANs), enable the creation of advanced threat detection frameworks capable of understanding nuanced human language and social behaviors online. By generating realistic synthetic data and simulating cyberattack scenarios, these models help train cybersecurity systems to identify subtle indicators of malicious activities like social engineering, disinformation campaigns, and hate speech propagation. This synthetic data augmentation is particularly valuable in overcoming data scarcity issues, allowing the detection systems to generalize better across diverse threat patterns.

Concrete examples are presented below, illustrating how generative AI supports each phase of cyber defense against social engineering, disinformation, and hate speech attacks. Table 1 summarises the examples.

- **Detection CSS**.
  Social Engineering. Generative AI models can produce synthetic phishing emails that mimic the language and style of recent campaigns. For example, by generating spear-phishing messages that incorporate personalized user data—such as recent social media activity or local events—security systems are trained on a richer dataset, improving their ability to detect subtle indicators of compromise in real-world attacks.
  Disinformation. Similarly, generative AI enables detection of disinformation by analyzing linguistic cues and inconsistencies in social media posts. For instance, it can detect emerging false narratives by comparing newly generated content with verified knowledge bases, flagging posts that deviate significantly in tone, factual accuracy, or style.
  Hate Speech. Generative models help identify novel slang, coded language, or context-dependent insults that traditional keyword-based filters may miss, thereby increasing the precision of automated moderation tools.
- **Response**.
  Social Engineering. When a phishing campaign is detected, generative AI assists incident response teams by simulating the attack progression and potential impacts, helping to prioritize mitigation actions. For example, it can generate likely phishing email variants to identify users at risk and tailor warning messages accordingly.
  Disinformation. In combating disinformation, generative AI can produce fact-checked counter-narratives and public awareness content in multiple languages and styles, accelerating the dissemination of corrective information. This was notably effective in simulated misinformation campaigns around health crises, where AI-generated responses improved public engagement and reduced rumor spread.
  Hate Speech. For hate speech outbreaks, generative AI aids moderators by drafting context-aware removal justifications and user communication, reducing response times and maintaining community trust.
- **Prevention**. *Social Engineering, Disinformation, Hate Speech.*
  Generative AI supports proactive defense by creating realistic attack simulations for training purposes. For instance, organizations have used AI-generated phishing emails that evolve dynamically, challenging employees with up-to-date social engineering tactics and improving their detection skills.

Additionally, generative AI can simulate emerging threat landscapes by producing hypothetical attack scenarios that blend new social trends and attacker tactics, enabling security teams to refine policies and deploy adaptive controls.
Finally, early warning systems enhanced with generative AI continuously analyze social media streams and generate predictive alerts about potential disinformation or coordinated hate campaigns before they escalate.

Table 1
Generative AI Applications in Cyber Social Security

Phase	Example Scenario	Generative AI Role	Impact
Detection	Personalized spear-phishing emails	Generate diverse synthetic phishing content for training detection models	Improved detection of subtle, targeted phishing attacks
	Emerging disinformation narratives	Analyze and generate text to identify linguistic anomalies and false narratives	Early flagging of false information and disinformation campaigns
	Novel hate speech patterns	Generate context-aware examples of evolving hate speech language	Enhanced moderation accuracy and reduced false negatives
Response	Phishing incident containment	Simulate attack variants and generate tailored warning messages	Faster risk prioritization and targeted user alerts
	Countering misinformation	Produce fact-checked, culturally adapted counter-narratives	Increased public awareness and mitigation of misinformation spread
	Hate speech moderation	Draft removal explanations and user communication	Reduced moderation response time and improved community trust
Prevention	Dynamic phishing simulations for training	Create evolving phishing email campaigns reflecting current social engineering tactics	Enhanced employee preparedness and resilience
	Threat landscape modeling	Generate hypothetical social engineering and disinformation scenarios	Proactive policy adjustments and improved adaptive defense
	Early warning alert generation	Analyze social data streams to predict and simulate coordinated attacks	Timely alerts and preemptive disruption of attack campaigns

5. Conclusion

It is a common viewpoint that the combination of data coming from social media, smartphones and from urban sensors can actually enable the ability to carry out in-depth analyzes and understand complex phenomena based on human behavior, opening new scenarios for the development of numerous innovative services and applications. By following this research line, the recent paradigm of Social Sensing further emphasized this vision, since it proposed an integrated model in which users themselves are turned into sensors, entities that produce simple rough information which is processed and aggregated in order to generate some valuable human-based findings obtained through the combination and merge of individual-based data. Beyond sensing applications, as those focusing on tracking vehicles to avoid traffic congestion or healthcare tracking and predicting people's lifestyles, a big research effort has been made to analyze text-based signals, such as those coming from social networks like X or Facebook. The reason is twofold: first, methodologies for Natural Language Processing (NLP) rely on very consolidated and effective algorithms, thus it is relatively simpler to process textual data rather than audio, video or especially environmental-based ones. Second, despite its size grows more slowly than video or audio data, textual content represents a very rich, interesting and valuable information source. Furthermore,

in a scenario where cyberspace events impact the real world and influence the political, social and cultural spheres, it is essential to have the cognitive, methodological superstructures as well as the cyber-physical infrastructures necessary to guarantee the resilience of civil society.

Therefore, this article presents a logical architecture for Cyber Social Security along both horizontal and vertical dimensions to enhance security across multiple domains. By integrating the five key CSS dimensions (i.e., Cyber Intimate Partner Violence, Cyber Gender-based Violence and Stereotype, Cyber Hate Speech and Falsehoods, Urban Mapping & Privacy, Ethical and Political Risks) with the critical security functions of Detection, Response, and Prevention, the proposed model enables a more dynamic and adaptive approach to face cyber social security threats.

In this context, the integration of Artificial Intelligence (AI) can enhance defense activities, accelerating the identification of potential social threats across CSS dimensions, increasing resilience and responsiveness of the social context. Future works concern a deeper investigation of Generative AI applications in CSS to further refine and expand this architecture.

Acknowledgment

This work was partially supported by the following projects: SERICS - “Security and Rights In the CyberSpace - SERICS” (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU; Patto territoriale "Sistema universitario pugliese" – CUP F61B23000370006.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] K. M. Carley, G. Cervone, N. Agarwal, H. Liu, Social cyber-security, in: R. Thomson, C. Dancy, A. Hyder, H. Bisgin (Eds.), Social, Cultural, and Behavioral Modeling, volume 10899 of *Lecture Notes in Computer Science*, Springer, Cham, 2018. doi:10.1007/978-3-319-93372-6_42.

[2] V. S. Barletta, M. Calvano, A. Sciacovelli, Cyber social security in multi-domain operations, in: 2024 IEEE International Workshop on Technologies for Defense and Security (TechDefense), 2024, pp. 41–46. doi:10.1109/TechDefense63521.2024.10863352.

[3] V. S. Barletta, D. Caivano, C. Catalano, M. de Gemmis, D. Impedovo, Cyber social security education, in: L. T. De Paolis, P. Arpaia, M. Sacco (Eds.), Extended Reality, Springer Nature Switzerland, Cham, 2024, pp. 240–248. doi:https://doi.org/10.1007/978-3-031-71713-0_16.

[4] M. T. Baldassarre, V. S. Barletta, D. Caivano, M. Scalera, Privacy oriented software development, Communications in Computer and Information Science 1010 (2019) 18 – 32. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85072844530&doi=10.1007%2f978-3-030-29238-6_2&partnerID=40&md5=2e236bb140c949fa89b00ef1fb2531bd. doi:10.1007/978-3-030-29238-6_2.

[5] B. Bhatti, Cyber security and privacy in the age of social networks, in: Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies, IGI Global, 2012, p. 18. doi:10.4018/978-1-60960-851-4.ch004.

[6] H. Aldawood, G. Skinner, Analysis and findings of social engineering industry experts explorative interviews: Perspectives on measures, tools, and solutions, IEEE Access 8 (2020) 67321–67329. URL: https://doi.org/10.1109/access.2020.2983280. doi:10.1109/access.2020.2983280.

[7] N. Sabar, X. Yi, A. Song, A bi-objective hyper-heuristic support vector machines for big data cyber-security, IEEE Access 6 (2018) 10421–10431. URL: https://doi.org/10.1109/access.2018.2801792. doi:10.1109/access.2018.2801792.

[8] A. Elmaghraby, M. Losavio, Cyber security challenges in smart cities: Safety, security and privacy, Journal of Advanced Research 5 (2014) 491–497. URL: https://doi.org/10.1016/j.jare.2014.02.006. doi:10.1016/j.jare.2014.02.006.

[9] M. T. Baldassarre, V. S. Barletta, D. Caivano, Smart program management in a smart city, in: 2018 AEIT International Annual Conference, 2018, pp. 1–6. doi:10.23919/AEIT.2018.8577379.

[10] D. Schatz, R. Bashroush, J. Wall, Towards a more representative definition of cyber security, The Journal of Digital Forensics, Security and Law (2017). URL: https://doi.org/10.15394/jdfsl.2017.1476. doi:10.15394/jdfsl.2017.1476.

[11] J. Orjatsalo, Facilitating cyber security threat modelling: A social capital perspective, in: European Conference on Knowledge Management, volume 23, 2022, pp. 878–884. URL: https://doi.org/10.34190/eckm.23.2.360. doi:10.34190/eckm.23.2.360.

[12] T. Tsikrika, B. Akhgar, V. Katos, S. Vrochidis, P. Burnap, M. Williams, 1st international workshop on search and mining terrorist online content & advances in data science for cyber security and risk on the web, 2017. URL: https://doi.org/10.1145/3018661.3022760. doi:10.1145/3018661.3022760.

[13] M. Senol, E. Karacuha, Creating and implementing an effective and deterrent national cyber security strategy, Journal of Engineering (2020) 1–19. URL: https://doi.org/10.1155/2020/5267564. doi:10.1155/2020/5267564.

[14] C. Onwubiko, K. Ouazzane, Challenges towards building an effective cyber security operations centre, International Journal on Cyber Situational Awareness 4 (2019) 11–39. URL: https://doi.org/10.22619/ijcsa.2019.100124. doi:10.22619/ijcsa.2019.100124.

[15] D. Lonsdale, The ethics of cyber attack: Pursuing legitimate security and the common good in contemporary conflict scenarios, Journal of Military Ethics 19 (2020) 20–39. URL: https://doi.org/10.1080/15027570.2020.1764694. doi:10.1080/15027570.2020.1764694.

[16] B. Green, M. Krotofil, A. Abbasi, On the significance of process comprehension for conducting targeted ics attacks, 2017. URL: https://doi.org/10.1145/3140241.3140254. doi:10.1145/3140241.3140254.

[17] K. Srivastava, A new approach of artificial intelligence (ai) to cyber security, International Journal of Research in Advent Technology 7 (2019) 410–412. URL: https://doi.org/10.32622/ijrat.71201980. doi:10.32622/ijrat.71201980.

[18] G. Christou, E. Papadogiannaki, M. Diamantaris, L. Torterolo, P. Chatziadam, Cybersure: A framework for liability based trust, in: Lecture Notes in Computer Science, Springer, 2020, pp. 19–34. URL: https://doi.org/10.1007/978-3-030-42051-2_2. doi:10.1007/978-3-030-42051-2_2.

[19] D. S. Reveron, Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, Georgetown University Press, Washington, DC, 2012.

[20] M. E. Bagwell-Gray, J. T. Messing, A. Baldwin-White, Intimate partner sexual violence: A review of terms, definitions, and prevalence, Trauma, Violence, & Abuse 16 (2015) 316–335.

[21] M. Breiding, K. C. Basile, S. G. Smith, M. C. Black, R. R. Mahendra, Intimate Partner Violence Surveillance: Uniform Definitions and Recommended Data Elements. Version 2.0, Technical Report, Centers for Disease Control and Prevention, 2015.

[22] J. Slupska, L. M. Tanczer, Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the internet of things, in: The Emerald International Handbook of Technology-Facilitated Violence and Abuse, Emerald Publishing Limited, 2021, pp. 663–688.

[23] E. L. Haines, K. Deaux, N. Lofaro, The times they are a-changing . . . or are they not? a comparison of gender stereotypes, 1983–2014, Psychology of Women Quarterly 40 (2016) 353–363. URL: https://doi.org/10.1177/0361684316634081. doi:10.1177/0361684316634081.

[24] J. Doughman, W. Khreich, M. E. Gharib, M. Wiss, Z. Berjawi, Gender bias in text: Origin, taxonomy, and implications, in: M. Lapata, H. Gonen, C. Hardmeier, K. Webster (Eds.), Proceedings of the 3rd Workshop on Gender Bias in Natural Language Processing, Association for Computational Linguistics, 2021, pp. 34–44. URL: https://aclanthology.org/2021.gebnlp-1.5. doi:10.18653/v1/2021.gebnlp-1.5.