Vilniaus universiteto leidykla

Contents lists available at Vilnius University Press

Information & Media
2026, vol. 104, pp. 38–54

eISSN 2783-6207
DOI: https://doi.org/10.15388/Im.2026.104.3

The Importance of Pop Culture and Media in Increasing Citizens' Cyber Defense Capacity: The Case of Estonia

Kate-Riin Kont

Estonian Academy of Security Sciences, Internal Security Institute
kate-riin.kont@sisekaitse.ee
https://orcid.org/0000-0002-9184-2363
https://ror.org/011fxed53

Abstract. While it is widely acknowledged that cyber risks can be managed and mitigated, they cannot be entirely eliminated. This reality underscores the importance of strengthening security awareness, fostering appropriate attitudes, and developing sound cyber hygiene from an early age. Such efforts not only reduce human error-related incidents but also help cultivate future cybersecurity professionals.

Cultural approaches may provide a particularly effective means of intervention. Cultural activities – ranging from theater, film, television, music, and literature – can reach diverse audiences and shape behavioral norms in ways that purely technical or informational campaigns often cannot. Although pop culture frequently exaggerates or dramatizes cybersecurity, it simultaneously plays a significant educational role, inspires future professionals, and reflects society's evolving relationship with technology. In Estonia, this relationship is particularly visible: cultural channels are increasingly used to promote cybersecurity awareness, reflecting a broader societal commitment to integrating technological development with reflective public discourse. The aim of this article is therefore to examine how popular culture can contribute to increasing citizens' cybersecurity awareness. In doing so, it extends existing cybersecurity discourse by situating digital safety within broader cultural practices, and arguing that pop culture can fill important gaps left by conventional awareness strategies.

Keywords: popular culture; cybersecurity awareness; cyber-specialist career; cybersecurity pop culture; cultural campaigns; media campaigns.

Popkultūros ir žiniasklaidos svarba didinant piliečių kibernetinės gynybos pajėgumus: Estijos atvejis

Santrauka. Nors plačiai pripažįstama, kad kibernetinės rizikos gali būti valdomos ir mažinamos, jų visiškai pašalinti neįmanoma. Ši realybė pabrėžia saugumo sąmoningumo stiprinimo, tinkamų nuostatų formavimo ir geros kibernetinės higienos ugdymo nuo ankstyvo amžiaus svarbą. Tokios pastangos ne tik mažina su žmogiškomis klaidomis susijusių incidentų skaičių, bet ir padeda ugdyti būsimus kibernetinio saugumo specialistus.

Kultūriniai požiūriai gali suteikti ypač veiksmingą intervencijos priemonę. Kultūrinės veiklos – nuo teatro, kino, televizijos, muzikos iki literatūros – gali pasiekti įvairias auditorijas ir formuoti elgesio normas taip, kaip to dažnai nepajėgia padaryti vien techninės ar informacinės kampanijos. Nors populiarioji kultūra dažnai perdeda ar dramatizuoja kibernetinį saugumą, ji kartu atlieka svarbų edukacinį vaidmenį, įkvepia būsimus specialistus ir atspindi kintantį visuomenės santykį su technologijomis. Estijoje šis santykis ypač akivaizdus:

Received: 2026-04-17. **Accepted:** 2026-05-11.

kultūriniai kanalai vis dažniau naudojami kibernetinio saugumo sąmoningumui skatinti, atspindint platesnį visuomenės siekį derinti technologinę pažangą su refleksyviu viešuoju diskursu. Todėl šio straipsnio tikslas – ištirti, kaip populiarioji kultūra gali prisidėti prie piliečių kibernetinio saugumo sąmoningumo didinimo. Taip plečiamas esamas kibernetinio saugumo diskursas, skaitmeninį saugumą įtvirtinant platesnių kultūrinių praktikų kontekste ir teigiant, kad populiarioji kultūra gali užpildyti svarbias spragas, kurias palieka tradicinės sąmoningumo didinimo strategijos.

Pagrindiniai žodžiai: popkultūra; kibernetinio saugumo sąmoningumas; kibernetinio saugumo specialisto karjera; kibernetinio saugumo popkultūra; kultūrinės kampanijos; medijų kampanijos.

Introduction: The Growing Cybersecurity Challenge

Compared to other Europeans, Estonians are among the most active daily Internet users. This high level of digital engagement raises a crucial question: how can the number of ordinary citizens falling victim to cybercrime be reduced? Cyberattacks, phishing scams, and data breaches frequently exploit human error, making individuals a central vulnerability in cybersecurity systems.

Globally, the frequency and sophistication of cyberattacks and cybercrime are increasing. The European Commission has noted that criminals have significantly benefited from technological progress, while institutional responses have not kept pace (European Commission, 2019). This imbalance is compounded by a severe shortage of cybersecurity professionals: in Europe alone, the shortage reached approximately 883,000 professionals in 2023, while, globally, the gap may have reached 13.5 million unfilled positions by 2025 (Cybersecurity Ventures, 2023). In Estonia, the shortfall was estimated at 870 specialists in 2023, representing an 86% increase in workforce demand. However, beyond the need for experts, there is an equally pressing need to improve cybersecurity competencies among citizens. Cybersecurity education should therefore be integrated into formal curricula across all educational levels (Pernik, 2019, 78).

Traditionally, awareness campaigns assume that providing information about risks will lead to behavior change. Such approaches often rely on fear-based messaging and instructions on threat avoidance (van Steen et al., 2020). Yet, research shows that these strategies may fail because they assume that users act as fully rational decision-makers, which is often not the case (Acquisti et al., 2015).

Cultural interventions offer an alternative by embedding cybersecurity knowledge within familiar narrative and emotional frameworks. Theater, film, literature, and exhibitions can help citizens understand risks in context and internalize safer practices. Nevertheless, *Estonia's Cultural Programme for 2023–2026* barely addresses cybersecurity, aside from assigning a limited role to public broadcasting as a crisis communication channel. Other cultural institutions are not formally included in cybersecurity awareness efforts. Rather than relying solely on fear-based messaging or technical instruction, cybersecurity education embedded in cultural forms can engage audiences more deeply, making risks and protective behaviors more relatable and memorable. Although pop culture frequently exaggerates or dramatizes cybersecurity, it simultaneously plays a significant

educational role, inspires future professionals, and reflects society's evolving relationship with technology. In Estonia, this relationship is particularly visible: cultural channels are being increasingly used to promote cybersecurity awareness, reflecting a broader societal commitment to integrating technological development with reflective public discourse. This article argues that systematic investment in cyber-related pop culture could contribute meaningfully to a safer digital future. At the same time, cyberpop culture remains underexplored globally, and, to the best of the author's knowledge, no prior study has examined its effects on cybersecurity capacity in the Estonian context.

At the same time, research emphasizes the need for coordinated national awareness strategies (Nagyfejeo & von Solms, 2020). Estonia has already integrated public libraries into cybersecurity campaigns, thus suggesting that broader cultural infrastructures could also be mobilized. This raises a key question: why not extend such efforts to theater, television, cinema, and literature as systematic components of cybersecurity education?

This research utilizes a multi-disciplinary framework with the objective to analyze the intersection of popular culture, media representation, and national cyber defense. The theoretical foundation is built upon Securitization Theory, and Media Framing (specifically, the 'Cyber-noir' aesthetic).

Securitization Theory and the Cyber-Landscape

A central concept in this study is the Copenhagen School's Securitization Theory, which explains how specific issues are moved from the realm of normal politics into the realm of security through 'securitizing moves'. In the Estonian context, cyber threats have been securitized not just as technical glitches but as existential threats to the 'e-state' and national identity (Ventsel & Madisson, 2019, 139).

Traditionally, cybersecurity has suffered from 'technification' – the reliance on expert authority that detaches the issue from public dialogue (Lacy & Prince, 2018). However, by linking security discourse with intertextual references to popular culture (such as science fiction or cyberpunk narratives), these complex threats become more 'tangible' for average citizens (Stritzel, 2012; Ventsel & Madisson, 2019). This study examines how popular culture helps transition cyber defense from a purely technical domain to a broader social and cultural dimension of national capacity building (Creese et al., 2021; Lacy & Prince, 2018).

Media Framing and the 'Cyber-Noir' Aesthetic

Cyberpop culture constitutes a broad category of cultural production that spans visual, textual, and electronic multimedia, including subgenres such as cyberpunk novels and films, comics and graphic novels, interactive computer games, visual arts, infomercials and computer advertisements, websites, and digital culture magazines (Matrix, 2006). As a genre, it plays a significant role in shaping identity formation and lifestyle by fusing technological ways of being with the integration of digital technologies into everyday

experience. Cyberpop culture thus functions as a creative interpretive space through which the effects of information and computer science on culture and individuals are explored, often challenging audiences to think differently about technological modernity.

Within this feedback loop of popular culture, cyberpop media – including advertisements, films, novels, and artworks – present provocative, imaginative, and frequently critical scenarios of present and future digital life (Matrix, 2006). As Matrix argues, "Cyberpop is a form of escapist mass media. Just like science fiction before it, today's cybercultural popular media genres often promote cyber and techno-literacy, help popularize high-tech aesthetics and communicate technoscientific imagery to the general public" (Matrix, 2006, 1–2). In this sense, cyberpop culture is not merely entertainment but also an informal educational infrastructure shaping technological imagination.

Despite its growing cultural relevance, the deliberate use of popular culture to inform broad populations about cybersecurity threats remains a relatively recent phenomenon that has received limited scholarly attention. Cyberpop culture includes diverse representations of cybersecurity topics across music, film, television, and literature, often depicting a dark underworld of digital risk that highlights the high stakes involved in protecting the digital sphere.

To understand how pop culture influences perception, this research draws on Media Framing and the concept of 'Cyber-noir'. Scholars commonly associate *noir* with themes of crime, greed, eroticism, pessimism, fatalism, moral ambiguity, and narrative closure that resists resolution (Walker-Morrison, 2018, 4–5). Within this lineage, cyber-noir emerges as a hybrid subgenre. Cybersecurity narratives frequently draw upon these aesthetics due to their alignment with uncertainty, hidden threats, and technological opacity. Popular media often depicts the digital world as a 'gloomy underworld' where threats are shrouded in moral ambiguity (Shires, 2019). This aesthetic, often found in films and novels, shapes the public's 'informal learning' and threat perception by personifying an abstract code into relatable villains or 'hacker' archetypes (Boholm, 2021; Shires, 2019).

As Shires concludes, although *noir* exaggerates darkness and moral ambiguity, cybersecurity narratives similarly rely on stylization: "the violence, catastrophe and glamour of cybersecurity is exaggerated, and deliberately so" (Shires, 2020, 101). Yet, this exaggeration does not diminish its educational potential. Contemporary film and television frequently integrate hacking narratives, sometimes accurately – and sometimes misleadingly. Films such as *WarGames* (1983) and *The Terminator* (1984) played a formative role in shaping public anxieties about machine autonomy and technological risk, with documented influence on policy development, including the US Computer Fraud and Abuse Act (Kaplan, 2017). *Noir* has also merged with science fiction in works such as *Blade Runner* (1982), which integrates dystopian futures with humanoid replicants, while cyberpunk narratives often blur the boundary between genres. Luhr (2012, 47), for example, uses the term 'tech-noir' to describe both *The Terminator* and *The Matrix* trilogy.

In Estonia, media coverage of cyber incidents – such as the 2017 ID card security risk or the Snowden scandal – often utilizes a 'discourse of fear', relying on analogies to help the public grasp intangible ICT risks. This study explores whether these pop-culture-ins-

pired frames can be leveraged to increase engagement rather than just fueling 'irrational anxiety' (Ventsel & Madisson 2019, 126).

International Precedents

The following literature review examines international precedents for integrating popular culture, television, music, and theater into national cybersecurity awareness strategies. Evidence from diverse global contexts suggests that these creative mediums are increasingly used to overcome the limitations of traditional, fear-based technical campaigns.

Cinema and Television: Narrative-Driven Engagement

In many foreign contexts, particularly the United States and Greece, cinema is viewed as a critical tool for both education and professional recruitment. In the U.S., prominent security figures – such as the former White House CIO Theresa Payton – emphasize that movies depicting hackers as ethical 'evildoers-fighters' are essential for engaging the next generation of talent. Iconic films like *WarGames* and *The Matrix* are frequently cited by industry leaders as the primary catalysts for their careers, demonstrating the power of pop culture to create a 'mission-driven' identity for future professionals (Morgan, 2022).

In Greece, research has explored the use of commercial movies in higher education to teach the principles of cybersecurity and cybercrime. Findings suggest that movies help students identify technical attack vectors and the psycho-social motivations behind social engineering in a way that traditional lectures cannot (Andreatos, 2020). By transforming abstract threats into high-stakes narratives, television series like *Mr. Robot* have been praised for their technical accuracy and their ability to educate the public on real-world hacking dangers (Morgan, 2022).

For example, *Mr. Robot* (2015–2019) and *Blackhat* (2015) are often cited as relatively informed portrayals of cyber threats, whereas other productions vary in technical accuracy. Even earlier films, such as *Ferris Bueller's Day Off* (1986) and *Ex Machina* (2014) embed implicit lessons about data protection, system vulnerabilities, and digital permissions. These examples demonstrate how pop culture simultaneously distorts and disseminates cybersecurity knowledge, while offering accessible entry points into otherwise complex technical domains.

The broader significance of such influence becomes particularly evident when considering gaps in formal education. Research showed that the UK school system provides insufficient IT education and limited exposure to cybersecurity careers, with 88% of surveyed adults reporting that they were unaware of cybersecurity as a career option during their schooling (Muncaster, 2017). In such contexts, popular culture assumes an especially important role. Nevertheless, at a societal level, cybersecurity remains underrepresented in mainstream cultural production, where television is often considered the most important medium.

Cybersecurity and Books

Literature remains a significant component of the cyberpop culture. Rick Howard (2014) proposes a distinction between two categories of hacker-themed books: those that rely on superficial or inaccurate representations of hacking, and those that attempt to portray technical processes and hacker culture realistically.

An example of the latter is *The Girl with the Dragon Tattoo* (2005), which is regarded by Howard as technically credible (Howard, 2014). The novel depicts detailed hacking activities performed by Lisbeth Salander, including encryption bypassing, malware installation, and financial system manipulation, situated within a realistic technological context of the early-2000s connectivity.

The challenge for cybersecurity-related fiction lies in balancing narrative engagement with technical accuracy. Before writing *The Girl in the Spider's Web* (2015), David Lagercrantz consulted cybersecurity expert David Jakoby so that to better understand hacking processes, including distinctions between malware types, vulnerabilities, and social engineering techniques. Their discussions emphasized that real-world hacking is a complex and time-consuming process, rather than the instantaneous activity commonly portrayed in fiction. The resulting novel reflects an effort to integrate authenticity into a narrative structure (Jakoby, 2015).

Howard (2014) further classifies Larsson's work as part of a 'canonical' cybersecurity reading list, suggesting that certain literary works can function as foundational educational texts for professionals (Patton, 2020). This underscores the pedagogical potential of literature when it engages seriously with technical domains.

Music and Rhythmic Campaigns: Cultural Localization

Nations in Asia and Africa have increasingly utilized music to make cybersecurity 'relatable' to younger demographics and non-technical users through local cultural genres.

India: In 2021, the Reserve Bank of India launched a major awareness campaign against cyber-fraud by collaborating with the Punjabi rapper *Viruss*. The campaign utilized rhythmic messaging to educate the public on common digital scams (Madhukalya, 2021).

Mongolia and Malta: Similar efforts were observed in Mongolia, where USAID partnered with local pop artists to release a rap song titled *My Online Information Is Mine* to promote data privacy (USAID, 2022). Whereas, in Malta, the Information Technology Agency integrated cybersecurity messaging into the high-profile Malta Song Contest to reach a broad domestic audience (NCC Malta, 2022).

Singapore and Nigeria: The Cyber Security Agency of Singapore utilized 'edutainment' music videos featuring marine life imagery (*Something's Phishy*) to teach anti-phishing skills to young adults (Tan et al., 2019). Meanwhile, in Nigeria, developers created the *Who Wants to Be Cybersecure?* app, which specifically utilized Afrobeats music and Pidgin English to increase the cultural resonance of security training for local users (Yisa & Orji, 2025).

Theater and Performance: Immersive Behavioral Simulation

Theater has emerged as a specialized medium for providing citizens with an 'embodied' experience of digital threats. In the United Kingdom, the educational theater project *Cyber Play* in Wales utilizes interactive theater for students in Years 9 and 10. By placing students within a narrative where they must make real-time decisions regarding phishing and malware, the project has demonstrated improved knowledge retention and a higher intention to practice secure behaviors (Teehan, 2025, 7918). Beyond the classroom, interactive theater performances are used internationally to simulate privacy crises (Skirpan et al., 2022). These simulations allow their participants to experience the emotional and ethical consequences of a data breach, which, as research suggests, is a more powerful motivator for behavioral change than passive reading (Aldaghlawy & Al-Shareeda, 2025; Skirpan et al., 2022).

The Awareness-Behavior Gap in Global Studies

Despite the creative success of these media-driven initiatives, international literature highlights a persistent 'awareness-behavior gap'. A study comparing internet users in Israel, Slovenia, Poland, and Turkey found that while awareness of threats is generally 'adequate', most citizens only implement the simplest protective measures (Zwilling et al., 2020). Researchers in the UK show systematic failure and note that many campaigns fail because they provide information without the psychological motivation or practical tools required to change long-term digital habits (Bada et al., 2019). This confirms that while pop culture is an excellent 'recruiter', it must be supported by formalized training so that to ensure technical effectiveness (Morgan, 2022; Zwilling et al., 2020).

Synthesis of International Findings

The global literature indicates that multimedia tools – including memes, infographics, quizzes, and videos – are significantly more effective at reaching 'high-priority' demographics like parents and children than the traditional text-based warnings (Rama & Keevy, 2023, 94; Zhang-Kennedy & Chiasson, 2021). The success of these foreign campaigns provides a critical benchmark for the Estonian case, suggesting that cultural engagement is a vital precursor to, but not a replacement for, professionalized technical defense (Bada et al., 2019; Rama & Keevy, 2023; Yisa & Orji, 2025).

Strategic Implementation in Estonia

Modern research has shifted from purely technical solutions to recognizing that cybersecurity is fundamentally a 'human factor' challenge (Jeong et al., 2021, 809). Scholars argue that since nearly half of all cybersecurity incidents result from human error, national resilience must be built upon a 'cybersecurity mindset' that is deeply embedded in social and cultural frameworks (Creese et al., 2021, 943). Culture, in this context, is defined as

the shared attitudes, beliefs, and values that dictate how individuals utilize cyberspace (Grobler et al., 2021). Traditional awareness campaigns often rely on 'fear-based' messaging or assuming that users will act rationally when provided with risk data (Acquisti et al., 2015). However, systematic reviews suggest that a more diverse range of media tools is more effective at engaging non-expert end-users (Zhang-Kennedy & Chiasson, 2021). Studies indicate that interactive and visual components, such as comics and cartoons, significantly improve the comprehension and memorization of security behaviors, which are otherwise viewed as 'boring and dry' (Sugatan, 2020, 11).

In Estonia, this holistic approach is reflected in how the government coordinates its defensive activities. The literature suggests that Estonia's use of popular culture is a world-class model for making cybersecurity 'visible' and 'relatable'. Cybersecurity capacity building is inherently shaped by social and cultural contexts (Creese et al., 2021). In Estonia, this is formalized through a Government Communication Handbook used to coordinate the detection of threats and the education of the public. This handbook specifically focuses on the detection and prevention of threats for educational purposes in schools and organizations, aiming to normalize 'cyber hygiene' as a routine aspect of digital life (Mölder et al., 2023, 102).

The European Union Agency for Cybersecurity (ENISA) coordinates the annual Cyber Awareness Campaign, supported by the European Commission, EU member states, Europol, the European Central Bank, EFTA countries, and over 300 public and private sector partners. This month-long initiative, which is held every October, provides up-to-date cybersecurity tips to help boost public confidence in Internet-based services and guide citizens on protecting their personal, financial, and work-related data online. Additionally, the NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) in Tallinn hosts its annual conference *CyCon*, organizes various technical training sessions (offered in English) and provides access to an e-library containing e-books, articles, reports, and videos on key cyber defense topics, along with additional training and exercise opportunities.

By framing cybersecurity within the familiar contexts of popular culture, the state aims to normalize 'cyber hygiene' as a civic duty. Data suggest that this approach is particularly effective in engaging the youth; for instance, the annual *KüberPähkel* survey, conducted since 2017, provides consistent indicative data on student competencies across four domains: privacy, technical savvy, problem-solving, and online behavior (Kont, 2023).

Estonia is recognized as an international leader in using diverse multimedia – such as memes, quizzes, and videos – on its government-led *Ole IT-vaatlik* platforms. These resources are strategically targeted toward high-priority groups like parents and children while serving the objective to ensure intergenerational awareness. During the *Be IT vigilant!* campaigns (2019–2020), public libraries acted as the primary dissemination points. Empirical results from 2020 show that this campaign led to the direct training of 44 library employees in Tallinn, equipping them with measurable skills in browser security, fraud recognition, and password management to serve as local experts. Furthermore, studies within academic environments, such as the Estonian Academy of Security Sciences,

confirm that formal training significantly improves cybersecurity behavior, particularly in the management of digital identities (Kont, 2024).

The aim of Estonia's Lifelong Learning Strategy 2014–2020 was to ensure that the competencies related to digital skills include cyber literacy and that, in addition to digital technology, basic knowledge related to cybersecurity is integrated into curricula. Starting with September 30, 2024, the Estonian National Broadcasting will air a weekly short program called *IT-aware* every Monday at 6:25 p.m. The show will introduce important cyber threats and provide advice on how to protect oneself. Topics will include the security of smart devices, recognizing scams, safe remote work and shopping, as well as many other useful tips. Despite these innovative efforts, research reveals significant gaps in formal implementation. A 2021-dated study on Estonian schools found that, although a curriculum for cybersecurity exists, 'cyber hygiene' is only actively taught in a few schools because institutions have the autonomy to choose their subjects (Bindevald, 2021). Consequently, many citizens turn to 'cybersecurity caregiving', relying on informal advice from friends and family. A study of 161 Estonian home users found that while this model is culturally accessible, it often lacks the 'accuracy and promptness' required for advanced defense, thus emphasizing the need for more formalized bridges between cultural engagement and professionalized support (Sein et al., 2026).

Estonia's strategic approach to cybersecurity emphasizes the human factor, integrating cultural, educational, and governmental efforts to build a strong 'cybersecurity mindset'. By combining formal policies with engaging media, popular culture, and community-based initiatives, Estonia makes cyber risks more understandable and relevant to everyday life. While these efforts have proven effective – especially in raising awareness and improving behavior among the youth – challenges remain in ensuring consistent formal education and bridging gaps between informal knowledge and expert-level cybersecurity practices.

Background of the Cultural Habits of Estonians

The role of culture in shaping a more secure digital future is not merely illustrative – it helps make abstract cyber threats understandable to people, influences attitudes, and can guide behavior. In the Estonian context, there are several strong examples where popular culture, media, and creative solutions support cybersecurity awareness and safety. At this point, it is essential to highlight why the influence of Culture on Estonian youth and adults may be greater than that of social media campaigns.

Among European countries, Estonia has the most museums per 100,000 inhabitants. The modern museum appeals to and offers activities for visitors of all ages, and Estonia's museums organize many educational programs, museum classes, virtual tours, movie programs and other events. Over time, the museums have developed into active centers of community and social life where both history and future enthusiasts meet. According to *Statistics Estonia*, in 2023, 174 museums at 229 locations were operating in Estonia. These were visited nearly 2.5 million times, which, in Estonia, amounts to 1,760 museum visits per thousand inhabitants.

Estonians are unmistakably a nation of readers. The culture of reading was strengthened during the Soviet era, when books were inexpensive and widely accessible. Reading was actively encouraged and became a way for Estonians to preserve their language and cultural identity. It was not unusual for people to purchase nearly every book that was published, resulting in impressively well-stocked home libraries (Saraste & Poikela, 2022). Even as the country has earned a global reputation as an IT powerhouse and a model for the digital age, its deep appreciation for books has remained remarkably strong. According to the latest Eurostat survey, Estonians spend more time reading than people in any of the 15 European countries studied. Finland comes in second, while France – somewhat unexpectedly – ranks last. Estonia is distinguished globally by an exceptionally high literacy rate of 99.87% and a deeply ingrained culture of print ownership. This strong tradition is reflected in the size of personal libraries; recent data (as of 2023) indicate that Estonian households possess an average of 218 books, which is a figure that ranks among the highest in Central and Eastern Europe (Pelău et al., 2023, 1083). Public libraries remain central to this reading habit, acting as critical institutional pillars where 50% of the population visits regularly.

People go to the cinema more and more in Estonia. A proof of that is the ever larger admittance numbers as well as a wide selection of films at the cinema. There are around 50 cinemas in Estonia with over 80 screens. In 2024, 446 (including 59 new Estonian films) new films in cinemas were screened in cinemas. There was 2.47 million cinema attendance accounted.

A very strong theater culture has developed in Estonia over the decades, even despite the current economic recession and ticket prices that sometimes seem ridiculously expensive (for example, tickets for a summer theater performance for a family of four can cost 222 euros and more, and this is in addition to the travel expenses that arise because summer performances happen away from the theatres' normal locations). There is also a long tradition of theater for young audiences, and the seasonal program of every theater necessarily includes both children's and youth performances. In addition to this, Estonia has the *Estonian Theatre for Young Audiences*, which also houses the *Museum of Puppetry Arts*. In 2023, more than 1.3 million people (1,327,980) went to Estonian theaters, with theaters giving 7,188 performances in total, including 716 different productions, 270 of which were new productions. In 2023, on average, Estonian theaters gave 19.6 performances per day, performances had 185 audience members, and a total of 3,632 spectators went to the theater per day (to compare, in 2019, the number was 3,489) (Estonian Theatre in Numbers, 2023, 2024). It cannot be stated that going to the theater is always the expressed desire of children and young people, but it is nonetheless important to instill in them the habit of going to the theater. According to studies from 2016 by the *Estonian Theatre Union* and the *Estonian Association of Performing Arts Institutions*, this is also reflected in the theaters' social media marketing: the younger the play's intended target audience, the more the marketing text is aimed at parents. Marketing aimed at teenagers, however, places the emphasis on teenagers' own agency. This kind of marketing also uses video material, slogans instead of long texts, and, overall, more 'youth-friendly' content (Kaalep, 2023).

From the above, we can see that Estonians have deeply rooted cultural habits such as active engagement in museums, reading, cinema, and theatre – which shape attitudes and behaviors and make culture a powerful channel for influencing societal awareness, including in the field of cybersecurity.

Popular Culture in the Service of a Safer Digital Future: Examples from Estonia

In Estonia, popular culture has increasingly become a meaningful medium for exploring and communicating the complexities of the digital world. Rather than addressing cybersecurity solely through technical or institutional channels, artists, writers, and media creators translate abstract technological developments into relatable human experiences. Through exhibitions, theatre, television, and literature, they engage audiences in reflecting on the opportunities and risks of digital life. The following examples illustrate how Estonian popular culture contributes to raising awareness, shaping attitudes, and fostering a more thoughtful and secure approach to the digital future.

An example of a cultural event in Estonia with a cyber-element is artist Timo Toots' longest-running and largest-scale installation, *Memopol* (2010). Toots has developed three versions of this installation, which collects information from the visitor's ID card, national databases and cell phone and then displays visualizations based on the collected data. While the users of the *Memopol-1* and *Memopol-2* installations were shown the information contained in their ID card or passport, *Memopol-3* added analyses of information obtained from the smartphone and cloud services. The *Memopol* exhibitions have traveled to many places across Europe, with the artist receiving wide recognition for the installations. In the words of Merilin Talumaa:

Timo Toots' activity could be characterized first of all by constantly researching technology and keeping it in focus. Although the technology around us is developing very quickly, its effects are generally still relatively little recognized. As a rule, the development of science is one step ahead of human reactions, which is why it is difficult to adapt to a situation of constant acceleration. The interactive installations of *Memopol* are also never finished but are in a constant process of changes and additions. It is possible to develop them further and lead the viewer to new interpretations. These are fictional stories that have potential applications and whose purpose is to make people relate to the surrounding environment in a dislocated way. (Talumaa 2019)

While the cultural events discussed so far and later in the paper mostly describe the connection between software and culture, the glass artist Rait Prääts' exhibition *CHIP CRISIS*, held in May 2022, explored the connection between hardware and culture. The artist suggests that a rapidly developing world of artificial intelligence has emerged within the natural world, giving birth to an augmented reality. Prääts' exhibition aims to explore and find connections and differences in this new world. He concludes that most pleasures and some temptations, too, belong only in the natural world. For example, in the artificial world, there is no abundance of smells, taste experiences, touches or enjoyment

of nature. At the same time, artificial intelligence's increasingly powerful entry into the evolution of the natural world is also noticeable. For example, people increasingly look at nature on a range of different screens. Augmented reality is a developmental leap that has brought many benefits but also a crisis of truth, an increasing desire for money, a crisis of ethics, hybrid wars, an energy crisis, a raw material crisis, a computer-chip crisis and the possibility of erasing everything at the push of a button. If we try to find something positive from the abovementioned crises, at least the chip crisis is significantly inhibiting the Russian Federation's aggression in the full-scale war in Ukraine, and there are signs that the high-tech aid received by Ukraine may help the country defend its independence. Putting that aside, augmented reality is undoubtedly here to stay and will continue to develop (Prääts, 2022).

The popular youth play *Born on the Net,* written by Kristiina Jalasto and staged by the *VAT Theatre*, was based on the performances of the real incidents on the Internet. The play was created in 2013 in cooperation between VAT and BCS Education as part of the *Theatre Online* project. It tells the story of young people who discover how connected and, though they differ, intertwined are the problems of the virtual and real world, and how many dangers and opportunities there are in the online environment that has become an integral part of our lives. The play's material was collected directly from young people through discussions about situations they have encountered in the virtual world. This was carried out in cooperation with the *Cybercrime Bureau of the National Criminal Police* and the *Estonian Union for Child Welfare*. From October 2013 to February 2014, *Born on the Net* was performed 32 times in different parts of Estonia, reaching approximately 11,000 audience members. The play was primarily intended for young people aged 12–16, and yet it offers much food for thought for teachers and parents as well. The audience's great interest and enthusiastic participation in the performances proved that theater performance is a form of culture extremely well-suited to having conversations about the dangers of the virtual world.

In Martin Algus's play *Something Real*, a dark story unfolds through the eyes of two characters which touches on the taboos of a nervous and anonymous modern society, in which, a person's pathological desire is counterbalanced by their longing for closeness and love. In 2019, a novel of the same name based on the play was awarded the annual literature prize of the *Estonian National Culture Foundation* and the *Eduard Vilde Literary Award*. *Something Real* is about two men: one, forced by circumstances, goes on a journey to a fast-food restaurant that is full of love and lust – the Internet, where a lonely person finds satisfaction for their bodily needs – the other, Karl, who has just been released from prison, starts looking on the Internet for help with his financial problems. In the background of all this, the show lightly, even humorously, presses questions about human desires that are still relevant in today's consumer and information society. The production is a *noir* world in both sound and image – a kind of adult cartoon world. In one of her interviews, the writer Jelena Skulskaja said about the play:

Kellerteater's *Something Real* shows that no matter how perfect the technology at our disposal is, at the bottom of the soul, man remains a primitive creature. When a per-

son is sick, he sits at the computer and escapes from trouble, even temporarily. He puts on headphones, faces the screen and can confess anything to this screen, like a doctor, psychologist or clergyman, even the most shameful and secret thing. (Skulskaja, 2022)

Directed by Margus Paju, the TV series *IT-planet*, an educational comedy, introduced topics related to computers and security in an entertaining way. The series was produced by the *Nafta* production house on behalf of the *Estonian Information System Authority* and was financed by the European Union Structural Funds program *Information Society Awareness Raising* to the amount of a fraction over 100,000 euros. The series, which includes a warning at the end of each episode about how one should or should not behave online, was well-received by critics. However, it had some detractors, with some finding it boring, difficult to follow and excessively moralizing. Piret Tali wrote the following about it:

All the prerequisites for the creation of a cult series were present: excellent producers and actors, but it seems that the subscriber could not keep himself in check. It seems that the subscribers did not have full confidence in the production company Nafta, whether pure art would still convey their worthy message. Or the creators of the series had no other excuse than the direct messages to present the cheerful movie as a popular science TV show. In both ways, the series is poorly substantiated and leaves a bloated impression. (Tali, 2011)

Published in 2022, the e-book *Print(memcpy[]): Stories of Estonian IT People* collects the stories of the Estonian IT people who rode the headwinds of the 1980s and 1990s to establish Estonian banks, telecoms, state institutions, IT companies and later, start-ups. The book contains thirty interviews with Estonian IT people. The author himself explains Estonia's IT-success as follows:

For some reason, in Estonia, IT people are trusted, they are involved in important decisions, and they are able to earn this trust. This kind of relationship has roots, and while thinking about them, I reached the time a little before and after the re-independence of the Estonian republic. When computers started to reach us back then, but the average person didn't have the ability to use them. And that's how the understanding that IT is useful and doing together makes sense was born. (Kütt, 2022, 11–12)

Given the discussion above, it can be affirmed that a culture has been created in Estonia, which articulates under the cyber pop culture – and some authors do this consciously, while others do so by writing, creating or mediating creations on a topic the topics that attract them most.

Conclusion

This article has examined the role of popular culture and media in strengthening citizens' cybersecurity awareness and, ultimately, national cyber defense capacity, by using Estonia as a case study. The study demonstrates that popular culture and media play a significant and increasingly strategic role in strengthening citizens' cyber defense capacity. In the Estonian context, cybersecurity is not treated solely as a technical or institutional issue but, rather, as a broader societal challenge shaped by cultural habits, narratives, and ev-

eryday practices. By embedding cybersecurity themes into familiar cultural forms – such as theater, literature, exhibitions, and television – complex digital risks become more accessible, relatable, and emotionally engaging for diverse audiences.

The Estonian case highlights how cultural engagement can complement formal cybersecurity strategies by fostering a 'cybersecurity mindset' rooted in shared values and behaviors. Estonia also serves as an example illustrating how these theoretical insights can be operationalized in practice. Estonia's strong cultural participation – which is evident in high levels of reading, museum attendance, cinema-going, and theatre engagement – creates a uniquely fertile environment for embedding cybersecurity awareness within everyday cultural experiences. Examples such as interactive exhibitions (e.g., *Memopol*), theatre productions (e.g., *Born on the Net*), noir-inspired narratives (*Something Real*), and educational media (*IT-planet*) demonstrate how cyber-related themes are already integrated into cultural production. These initiatives align closely with both securitization processes (by reinforcing cybersecurity as a societal concern) and media framing dynamics (by shaping how risks are perceived and understood). From a media framing perspective, the 'cyber-noir' aesthetic demonstrates how dramatized and stylized representations – despite their exaggerations – play a significant role in shaping public perception and informal learning. These narratives frame cyberspace as uncertain, risky, and morally ambiguous, thereby reinforcing its status as a security domain while simultaneously engaging audiences emotionally. From a securitization perspective, cybersecurity in Estonia has been successfully elevated to a matter of national importance; however, the 'technification' of the field risks distancing citizens from active participation. Popular culture helps bridge this divide by translating abstract threats into socially meaningful narratives, thereby making cyber risks more tangible and relatable.

At the same time, the findings confirm that while popular culture is highly effective in raising awareness and motivating interest, it cannot fully replace structured education and professional training. The persistence of gaps between awareness and behavior indicates the need for stronger integration between cultural initiatives and formal cybersecurity frameworks.

Overall, Estonia provides a compelling example of how a digitally advanced society can leverage its rich cultural environment to support cybersecurity goals. Continued and more systematic investment in cyber-related popular culture – alongside institutional and educational measures – can contribute to building a more resilient, informed, and security-conscious society.

References

2022 Rait Prääts KIIBIKRIIS HOP galeriis. Eesti Klaasikunstnike Ühendus, 2022. https://klaasikunst.ee/?p=5981

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Aldaghlawy, H. J., & Al-Shareeda, M. A. (2025). The role of simulating digital threats through interactive theater performances. *Journal of Cyber Security and Risk Auditing*, *2025*(4), 276–286. https://doi.org/10.63180/jcsra.thestap.2025.4.7

Andreatos, A. (2020). Movies as an aid to teach principles of Cybersecurity and Cybercrime in Higher Education. *International Journal of Education and Information Technologies*, *14*, 76–82. http://doi.org/10.46300/9109.2020.14.10

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). *Cyber security awareness campaigns: Why do they fail to change behaviour?* arXiv:1901.02672. https://doi.org/10.48550/arXiv.1901.02672

Bindevald, A. (2021). *Küberturvalisus koolides – väljakutsed, võimalused ja vajadused CTF-lahenduse järele. Cyber Security at Schools – Challenges, Opportunities and Needs for CTF-Solution* [Master's thesis, Tallinna Tehnikaülikool]. https://digikogu.taltech.ee/et/Item/49f9674f-34c7-4db6-a938-25738dd2d61f

Boholm, M. (2021). Twenty-five years of cyber threats in the news: a study of Swedish newspaper coverage (1995–2019). *Journal of Cybersecurity*, *7*(1), Article tyab016. https://doi.org/10.1093/cybsec/tyab016

Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions. *Personal and ubiquitous computing*, *25*(5), 941–955. https://doi.org/10.1007/s00779-021-01569-6

Cybersecurity Ventures. (2023). *Official Cybersecurity Jobs Report*. https://newsletter.radensa.ru/wp-content/uploads/2023/11/2023_OfficialCyberSecurity_JobsReport.pdf

Eesti Kultuuriprogramm 2023–2026. Kultuuriministeerium, 2023. https://kul.ee/media/4318/download

Estonian Theatre in Numbers 2022. (2023). https://teater.ee/eesti-teatri-agentuur/valjaanded/estonian-theatre-in-numbers-2022/

European Commission. (2019). *Cybercrime. Migration and Home Affairs*. https://ec.europa.eu/home-affairs/what-wedo/policies/organized-crime-and-human-trafficking/cybercrime_en

Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage and usability: Redefining human centric cyber security. *Frontiers in Big Data*, *4*, Article 583723. https://doi.org/10.3389/fdata.2021.583723

Howard, R. (2014, March 26). The cybersecurity canon: The girl with the dragon tattoo. *Palo Alto Networks.* https://www.paloaltonetworks.com/blog/2014/03/cybersecurity-canon-girl-dragon-tattoo/

Jakoby, D. (2015, August 27). Hacking a book: how I became Lisbeth Salander. *Kaspersky*. https://www.kaspersky.com/blog/hacking-girl-with-dragon-tattoo/9651/

Jeong, J. J., Oliver, G., Kang, E., Creese, S., & Thomas, P. (2021). The current state of research on people, culture and cybersecurity. *Personal and ubiquitous computing*, *25*(5), 809–812. https://doi.org/10.1007/s00779-021-01591-8

Kaalep, E., Juhkam, K., & Miilman, E. (2023, February). Loomingulisest beebist agentse teatrivaatajani. *Teater. Muusika. Kino*. https://www.temuki.ee/archives/7209

Kaplan, F. (2017). *Dark Territory: The secret history of cyber war.* Simon & Schuster.

Kont, K. R. (2023). Cyber literacy skills of Estonians: activities and policies for encouraging knowledge-based cyber security attitudes. *Information & Media*, *96*, 80–94. https://doi.org/10.15388/Im.2023.96.67

Kont, K. R. (2024). Cybersecurity behaviours of the employees and students at the Estonian Academy of Security Sciences. *Organizational Cybersecurity Journal: Practice, Process and People*, *4*(2), 85–104. https://doi.org/10.1108/OCJ-02-2024-0001

Kütt, A. (2022). *Print(memcpy[]): Eesti IT-inimeste lugusid*. TeamCosulting OÜ. https://media.voog.com/0000/0049/9532/files/memcpy_digital.pdf

Luhr, W. (2012). *Film Noir.* Wiley-Blackwell.

Madhukalya, A. (2021, February 22). RBI ropes in Punjabi rapper for awareness campaign on cyber fraud. *Business Today*. https://www.businesstoday.in/latest/economy-politics/story/rbi-ropes-in-punjabi-rapper-for-awareness-campaign-on-cyber-fraud-289002-2021-02-22

Matrix, S. E. (2006). *Cyberpop. Digital Lifestyles and Commodity Culture.* Routledge.

Morgan, S. (2022, April 13). Pop culture is cybersecurity's best recruiter. *Cybercrime Magazine*. https://cybersecurityventures.com/pop-culture-is-cybersecuritys-best-recruiter/#:~:text=Pop%20culture%20has%20been%20recruiting,calling%20after%20watching%20a%20movie

Muncaster, P. (2017, October 19). UK cybercrime falls but stats are still shaky. *Infosecurity Magazine*. https://www.infosecurity-magazine.com/news/uk-cybercrime-falls-but-stats-are

Mölder, H., Chochia, A., & Nyman-Metcalf, K. (2023). Elite Agenda, Media Framing, and Public Perception of European Integration in Estonia. *TalTech Journal of European Studies*, *13*(2), 63–110. https://doi.org/10.2478/bjes-2023-0016

Nagyfejeo, E., & von Solms, B. (2020). Why do national cybersecurity awareness programmes often fail? *International Journal of Information Security and Cybercrime*, *9*(2), 18–27. https://doi.org/10.19107/IJISC.2020.02.03

NCC Malta. (2022, January 27). *Cyber Security Launches Campaign with Malta Song Contest*. https://ncc-mita.gov.mt/news/cyber-security-launches-campaign-with-malta-song-contest/

Patton, H. (2020, August 6). The Cybersecurity Canon: A Resource for Security Professionals Comes to Higher Education. *Security Matters* (blog), *EDUCAUSE Review*. https://icdt.osu.edu/cyber-canon/about-cybersecurity-canon

Pelau, C., Ghinea, V., & Hrib, B. (2023). Social Image in the Online Environment–Sustainable Motive for Book Sales During the Pandemic. *Amfiteatru Economic*, *25*(17), 1081–1094. https://doi.org/10.24818/EA/2023/S17/1081

Pernik, P. (2019). Cybersecurity education in Estonia: Building competences for internal security personnel. In *Proceedings, XVIII, 2019 Security: From corner to corner* (pp. 71–108). https://digiriiul.sisekaitse.ee/bitstream/handle/123456789/3122/Cybersecurity%20education.pdf?sequence=1&isAllowed=y

Rama, P., & Keevy, M. (2023). Public cybersecurity awareness good practices on government-led websites. *International Journal of Research in Business and Social Science*, *12*(7), 94–104. https://doi.org/10.20525/ijrbs.v12i7.2840

Saraste, P., & Poikela, S. (2022, September 12). The passion for reading is still strong in Estonian. *The Baltic Guide*. https://balticguide.ee/en/the-passion-for-reading-is-still-strong-in-estonian/

Sein, K., Sütterlin, S., & Mällo, T. (2026). Cybersecurity-related support needs and challenges incurred by informal support: a study among Estonian home users. *Journal of Cybersecurity*, *12*(1), Article tyag006. https://doi.org/10.1093/cybsec/tyag006

Shires, J. (2020). Cyber-noir: Cybersecurity and popular culture. *Contemporary Security Policy*, *41*(1), 82–107. https://doi.org/10.1080/13523260.2019.1670006

Skirpan, M., Oates, M., Byrne, D., Cunningham, R., & Cranor, L. F. (2022). Is a privacy crisis experienced, a privacy crisis avoided?. *Communications of the ACM*, *65*(3), 26–29. https://doi.org/10.1145/3512325

Skulskaja, J. (2022, June 13). Arvustus. Kas on olemas tõelisus väljaspool arvutimaailma? *Eesti Päevaleht.*

Sugatan, C. (2020). *The Design and Development of an Interactive Story for Security Education: A Case Study on Password Managers*. University of Michigan.

van Steen, T., Norris, E., Atha, K., & Joinson, A. (2020). What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity*, *6*(1), Article tyaa019. https://doi.org/10.1093/cybsec/tyaa019

Tali, P. (2011, March 30). "IT-planeet" ripub kahe tooli vahel. *Eesti Päevaleht*. https://epl.delfi.ee/artikkel/51294528/it-planeet-ripub-kahe-tooli-vahel. Accessed 28 Oct. 2023

Tan, A. Y., Chng, C. Y. Z., Oh, C. Y., & Gan, P. Q. (2019). *Something's phishy: a communications campaign designed to teach young adults to combat phishing threats*. Nanyang Technological University. https://dr.ntu.edu.sg/entities/publication/d69c2982-fddf-4609-8b58-dac9fb910f1f

Talumaa, M. (2019, December 11). Timo Tootsi tagurpidi ideed ajamasinas. *Müürileht*. https://www.muurileht.ee/timo-tootsi-tagurpidi-ideed-ajamasinas/

Teehan, C. (2025). Cyber Play: a narrative-driven approach to cybersecurity education for pre-GCSE learners. In *ICERI2025 Proceedings* (pp. 7918–7924). IATED. https://doi.org/10.21125/iceri.2025.2207

USAID. (2022). *USAID launches cybersecurity awareness campaign in Mongolia*. https://www.usaid.gov/asia-regional/press-releases/feb-28-2022-usaid-launches-cybersecurity-awareness-campaign

Ventsel, A., & Madisson, M. L. (2019). Semiotics of threats: Discourse on the vulnerability of the Estonian identity card. *Sign Systems Studies*, *47*(1/2), 126–151. https://doi.org/10.12697/SSS.2019.47.1-2.05

Walker-Morrison, D. (2018). *Classic French noir: Gender and the cinema of fatal desire*. I.B. Tauris. https://books.google.ee/books?hl=en&lr=&id=GRKEDwAAQBAJ&oi=fnd&pg=PP1&ots=LrMz5EJNNc&sig=SbBv4DAMKba1tFhHQ_W9OBhIqik&redir_esc=y#v=onepage&q&f=false

Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)*, *54*(1), 1–39. https://doi.org/10.1145/3427920

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Yisa, V. L., & Orji, R. (2025, November). Who Wants to Be Cybersecure? Expert Evaluation of a Culturally Adaptive Gamified Cybersecurity Awareness App. In *Proceedings of the 5th Biennial African Human Computer Interaction Conference* (pp. 243–255). https://doi.org/10.1145/3757232.3757249