# Censorship in Cybersecurity and its Effect on the Shortfall of Cybersecurity Professionals

Lotus Virtual Laboratories, Storm AI

## Table of Contents





## summary

Censorship in cybersecurity encompasses the regulation and restriction of information related to online threats, impacting both the knowledge available to cybersecurity professionals and the broader state of cybersecurity practices. This phenomenon is particularly significant in the context of rising cyber threats and the global shortage of cybersecurity experts, with estimates suggesting a deficit of nearly 4 million skilled professionals worldwide.[1][2] The interplay between censorship and the availability of cybersecurity content has sparked notable debate regarding its implications for national security, privacy rights, and the development of a competent workforce.

While proponents argue that censorship can safeguard national security by mitigating risks associated with terrorism and cyberattacks, critics highlight the adverse effects on knowledge dissemination and professional growth within the cybersecurity community.[3][4] The restrictions on access to crucial information—including methodologies for combating cyber threats—can hinder the ability of professionals to innovate and respond effectively to evolving challenges. Furthermore, self-censorship among practitioners, driven by fear of retribution, stifles open communication and collaboration, exacerbating the shortage of qualified individuals in the field.[5][6]

Commercial filtering tools, which are often implemented to enhance user safety, can unintentionally restrict access to essential cybersecurity resources, limiting educational opportunities for both current and aspiring professionals.[6][7] As organizations increasingly rely on digital technologies, the demand for skilled cybersecurity personnel has surged; however, censorship practices may impede the training and development necessary to meet this demand.[8][9] The ramifications of this censorship extend beyond immediate security concerns, threatening the future resilience of the cybersecurity workforce and the ability to safeguard critical digital infrastructures.

In summary, while the intention behind censorship may be to enhance security, it poses significant challenges to the cultivation of cybersecurity expertise. By creating barriers to information access and fostering a culture of avoidance, censorship not only hampers innovation but also contributes to the persistent shortage of cybersecurity professionals essential for navigating the complexities of the digital landscape.[1][10]

# Censorship in Cybersecurity

Censorship in the field of cybersecurity plays a multifaceted role, influencing both the landscape of information available to cybersecurity professionals and the overall state of cybersecurity practices. It involves the regulation of content related to online threats, which can range from harmful software to potentially illegal activities. This censorship can have significant implications for the understanding and development of effective cybersecurity measures.

## National Security and Censorship

Censorship can be justified in certain contexts as a means to protect national security from online threats such as terrorism, cyber espionage, and cyberattacks. By restricting access to harmful content, organizations aim to create a safer digital environment

for users, ensuring that malicious actors are unable to exploit vulnerabilities within the cybersphere[1][3]. However, this practice raises concerns about the balance between security and privacy rights. Modern cybersecurity solutions must navigate this delicate balance to protect users while respecting their freedoms[4][3].

## Impact on Cybersecurity Knowledge and Awareness

The censorship of cybersecurity-related content also impacts the dissemination of knowledge within the field. For instance, restrictions on information regarding internet censorship methodologies, network traffic obfuscation, and related human aspects hinder the ability of cybersecurity professionals to effectively understand and counteract various threats. A lack of comprehensive studies and surveys on these topics means that vital information is often not accessible to those who need it most[5][3].

Furthermore, self-censorship among individuals can occur due to fear of repercussions, which can stifle innovation and communication within the cybersecurity community. Professionals may limit their expressions or refrain from sharing critical insights that could contribute to collective knowledge, further exacerbating the shortage of expertise in the field[1][6].

## Societal Implications and the Role of Commercial Filtering

Censorship also extends to the use of commercial filtering software, which, while designed to protect users, may inadvertently limit access to crucial cybersecurity resources. The sophistication of online content filtering has grown due to the involvement of companies from various nations, potentially leading to a homogenized and restricted flow of information in the cybersecurity sector[6]. This can hinder the training and development of new cybersecurity professionals, contributing to the ongoing shortage in the workforce.

Ultimately, the intersection of censorship and cybersecurity highlights a complex challenge: while the intent behind censorship may be to secure digital spaces, it also risks stifling innovation and limiting access to knowledge, thus contributing to the shortage of qualified cybersecurity professionals.

# Impact of Censorship on Cybersecurity Professionals

Censorship within the cybersecurity domain has significant implications for the development and retention of cybersecurity professionals. By restricting access to information and limiting educational resources, censorship can create knowledge gaps that hinder the growth of individuals in this critical field. This limitation not only affects the quality of education but also restricts the innovation and adaptability needed to address evolving cyber threats effectively[7][8].

## Limitation of Educational Resources

Heavily censored environments often prevent students and professionals from accessing essential global news, advanced training materials, and educational resources that are vital for understanding the complexities of cybersecurity[8]. This restricted access poses a direct threat to the educational opportunities available to future cybersecurity experts, resulting in a workforce that is ill-prepared to tackle sophisticated cyber challenges. Furthermore, such limitations can stifle interest in cybersecurity careers, as individuals may not have the exposure to necessary skills and knowledge that would spark their interest in the field[11].

### Culture of Avoidance

The culture of censorship can also lead to a workplace environment where professionals feel discouraged from discussing critical issues related to cybersecurity. Employees may develop a fear of retribution for voicing concerns or suggesting new ideas, which can result in self-censorship and a lack of innovation[12][10]. This culture of avoidance ultimately weakens the cybersecurity workforce, as it discourages the open exchange of ideas and reduces collaboration among team members, leading to stagnation and a failure to adapt to new threats.

### Talent Retention Challenges

As cybersecurity professionals are in high demand, organizations must create an environment that fosters support, learning, and open communication. However, censorship can create barriers to building a strong workforce. If employees feel that their voices are not heard, or that they are unable to challenge outdated practices, they are more likely to leave for organizations that promote a more inclusive and open culture[9][10]. Consequently, this can exacerbate the existing talent shortage in the cybersecurity industry, making it even more challenging for organizations to secure their digital environments effectively.

## The Cybersecurity Professional Shortage

The cybersecurity professional shortage is a significant challenge facing organizations globally, exacerbated by a rising demand for skilled professionals amid increasing cyber threats. Over two thirds of organizations (67%) report some form of shortage of cybersecurity professionals within their teams[2]. The global skills deficit is estimated to be nearly 4 million cybersecurity experts, a figure projected to grow as the demand for cybersecurity expertise continues to escalate[13].

### Factors Contributing to the Shortage

#### Increased Demand for Cybersecurity Talent

The demand for cybersecurity talent has surged exponentially in recent years due to the escalating number of cyberthreats. As businesses expand their digital operations and embrace digital transformations, the necessity for qualified cybersecurity pro-

fessionals to safeguard these technologies has become increasingly critical[14][15]. Despite the global cybersecurity workforce growing to 4.7 million individuals—its highest level ever—there remains a need for over 3.4 million additional professionals to effectively mitigate risks and manage threats[9].

### Limited Recruitment Practices

One factor contributing to the shortage is the restrictive nature of many organizations' recruitment practices. Frequently, job postings for cybersecurity positions emphasize traditional educational credentials, such as degrees in technology-related fields, which can deter potential candidates from diverse backgrounds who may possess valuable skills and innovative ideas[16]. To combat this shortage, organizations are encouraged to broaden their recruitment strategies to include non-traditional candidates who can contribute unique perspectives and solutions to cybersecurity challenges.

### Rising Cybersecurity Threats

The increasing frequency and sophistication of cyberattacks further underline the urgent need for skilled professionals. Projections suggest that spending on cybersecurity services will reach $101.5 billion by 2025, while the costs associated with cybercrime are expected to rise by 15 percent, reaching an alarming $10.5 trillion[15][3]. This heightened awareness of cybersecurity threats is driving more organizations to seek qualified professionals to help them navigate these challenges.

## Consequences of the Shortage

The lack of cybersecurity professionals not only compromises an organization's ability to defend against cyber threats but also poses significant risks to client trust and operational integrity. Without a robust team of cybersecurity experts, organizations may struggle to adequately service their clients and protect against the increasing risks posed by cybercriminals[9][17].

# Case Studies

## Impact of School Web Filtering

The consequences of web filtering in educational environments illustrate a significant challenge to access information crucial for cybersecurity education. Nearly every school in the United States employs automatic web filters, primarily due to the mandates set by the Children’s Internet Protection Act (CIPA) passed in 2000. This law requires schools and libraries to block access to “child pornography” and other content considered “obscene” or “harmful to minors” to qualify for federal technology funding, known as E-rate funding[6][18]. In districts like Albuquerque, substantial investments have been made to provide students with take-home computers, yet these filters have increasingly dictated their online experiences, both in and out of

school[6][19]. The restrictions imposed can prevent students from accessing vital cybersecurity resources, training materials, and discussions that are essential for developing a skilled workforce in this critical field.

## Trust and Participation in Measurement Studies

The success of cybersecurity measurement studies and tools is closely tied to public trust in their security and reliability. If individuals lack confidence in these tools, their willingness to participate in measurement studies diminishes, hindering data collection that is essential for understanding and addressing cybersecurity issues[20][21]. This lack of engagement can further exacerbate the shortage of cybersecurity professionals, as educational institutions and training programs may struggle to acquire the necessary data to tailor their curricula effectively.

## Censorship and Control in Corporate Policies

Corporate policies on content moderation and censorship significantly influence the dissemination of cybersecurity knowledge. Engaging in continuous dialogue with civil society is crucial for understanding how these policies impact users' access to information. Companies operating in various markets, especially those with unique human rights challenges, must consult local expertise to ensure that their policies do not inadvertently suppress vital cybersecurity content. This is particularly important during sensitive times, such as elections or crises, where the need for accurate information is paramount[22][11][23]. Failure to provide open access to cybersecurity information may contribute to the ongoing professional shortage, as potential talent remains uninformed or misinformed about career opportunities and essential skills in the field.

# References


[1]: Pros and cons of internet censorship: All you need to know - NordVPN
[2]: Journalists & Cyber Threats
[3]: [PDF] The Sociological Effects of Censoring Public AI
[4]: How We Investigated Web Censorship in Schools - The Markup
[5]: Security and Censorship - Ithaka S+R
[6]: AI Isolationism's Risks: The Unintended Consequences of Banning ...
[7]: How Internet Censorship Impacts Society and Online Freedom
[8]: [PDF] The State of Cybersecurity Education in K-12 Schools - Cyber.org
[9]: Choke points and censorship: Protecting free flow of ... - ASU News
[10]: Impacts of Censorship in the Workplace | AJE
[11]: [PDF] CYBERSECURITY AND HUMAN RIGHTS - Global Partners Digital
[12]: Employers Must Act as Cybersecurity Workforce Growth Stalls and ...
[13]: Why closing the cyber skills gap requires a collaborative approach
[14]: Internet Censorship and Libraries - ALSC Blog

[15]: Internet Censorship (Part 2): The Technology of Information Control
[16]: Cybersecurity for Civil Society: A Case Study - IRI
[17]: Policy Recommendations: Internet Freedom
[18]: Digital censorship in democratic nations. New York becomes first ...
[19]: Inside America's School Internet Censorship Machine - WIRED
[20]: Protecting Human Rights on the Internet - Amnesty International
[21]: What the Fight Against Classroom Censorship is Really About - ACLU
[22]: Circumventing Censorship of Social Media and Online Content in a ...
[23]: Censorship or Safety: Should Schools Use Content Filtering Software?