ESCP
BUSINESS SCHOOL

IT ALL STARTS HERE

BERLIN | LONDON | MADRID | PARIS | TURIN | WARSAW

© Irissca-AdobeStock

LIGHTS - Human/Well being

Cybersecurity: is the human factor its center of gravity?

ESCP Impact Paper No.2025-26-EN

Bastian DUFILHOL
ESCP Business School

ESCP RESEARCH INSTITUTE OF MANAGEMENT (ERIM)

ESCP Impact Paper No.2025-26-EN

Cybersecurity: is the human factor its center of gravity?

Bastian Dufilhol*

ESCP Business School

Abstract

Today, with 80% of successful cyberattacks exploiting human error, threats are structured across a continuum of cyber, digital, informational, and cognitive domains, whether institutional and aimed at destabilization, criminal in nature, or a hybrid via proxies acting on behalf of governments. This continuum thrives in an ecosystem where social engineering is the primary mode of action, relying on data capture and the ability to influence behaviors, either individually, through pressure tactics, or collectively, as in mass manipulation. Personal data has thus become raw material. In this context, the paradigm shift lies in the fact that the human factor has now become the main vector of threat. The main implication is that the field of cyber vulnerability for an organization is no longer its own systems, but the ecosystem of its people, which is much more complex to control and presents unknown risks that are both difficult to quantify and to mitigate. The paths to explore for a structured response might include strong executive sponsorship, cybersecurity cross-functionality, information sharing, integration of digital, informational, and communication domains, comprehensive human factor considerations, and dual capabilities, to both protect and act within the cyber–digital–informational–cognitive continuum, fostering a broader continuum of security.

Keywords: cybersecurity, human factors, security continuum, threat intelligence, social engineering.

*Professor, ESCP Business School, Executive Director ESCP Branch Campus – Dubai (UAE)

Cybersecurity: is the human factor its center of gravity?

In May 2024, several European parliamentary assistants were targeted by a particularly sophisticated social engineering campaign. Cybercriminals used convincingly fake LinkedIn© profiles to connect with these staffers, offer them appealing career opportunities, and ultimately lure them into opening malicious documents or disclosing sensitive information. A textbook case of a 100% cognitive *modus operandi*, with overlapping political and economic goals, and a direct exploitation of the targets' digital footprint.

The root "cyber" comes from the term "cybernetics," coined in French in 1834 to refer to the "science of government," derived from the Greek *kubernêtiké*, meaning "to steer, govern." The term was reintroduced in 1948 in the United States by mathematician Norbert Wiener, the founder of cybernetics, the science encompassing theories of control, regulation, and communication between living beings and machines.[1] Even before the emergence of what has been known since 1984[2] as cyberspace, the human factor, in all its dimensions, has been fundamentally central.

Today, with 80% of successful cyberattacks exploiting human error, **threats are structured across a continuum of cyber, digital, informational, and cognitive domains**, whether institutional and aimed at destabilization, criminal in nature, or a hybrid via proxies[3] acting on behalf of governments.

This continuum thrives in an ecosystem where social engineering is the primary mode of action, relying on data capture and the ability to influence behaviors, either individually, through pressure tactics, or collectively, as in mass manipulation. Personal data has thus become raw material. In this context, the paradigm shift lies in the fact that the the vector of the threat is now the human factor.

This raises the following question: should cyber defense, likely still too fragmented, also operate within this continuum to ensure effective protection? Moreover, for both individuals and organizations, mastering their digital footprint now seems crucial to counter this threat.To understand the weight of the human factor and the concepts of direct and indirect strategies, the starting point is an assessment of social engineering attacks. For a holistic approach, this must be complemented by a psychological and behavioral analysis of the threat. In an increasingly asymmetric battlefield, notably for legal reasons, personal data stands out for its uniqueness, sensitivity, and its transformation into a unit of value. Based on these findings, we can begin outlining avenues for structuring cyber defense in a continuum already exploited by adversaries.

Social engineering attacks have become the preferred course of action

First and foremost, we must examine the cyber kill chain, the value chain of cyber threats, which benefits from a highly favorable ecosystem of hybridization between personal and professional digital lives. Based on research and insights from ANOZR WAY[4], this chain comprises several steps. First, an organization is selected for its strategic interest (espionage, proxy use, destabilization leverage, etc.). Next, high-value individuals are

[1] Solange Ghernaouti, Cybersecurity, 7th edition, DUNOD

[2] William Gibson is an American writer inspired by the countercultures of the 1970s and 1980s. He has authored numerous visionary science fiction novels. He mentioned cyberspace for the very first time in his book *Neuromancer* in 1984.

[3] In the context of conflict, a proxy refers to an organization or group acting on behalf of a government without an official or direct affiliation.

[4] ANOZR WAY is a French startup, created in 2025, specialized in cyber risk management through human factor approach and digital footprint awareness and vulnerabilities reduction.

identified: executives, personnel in sensitive roles, and anyone with high cyber exposure. Cyber exposure is defined as the combination of vulnerabilities and attack surface based on one's digital footprint.[5] Once these individuals are identified, data is gathered from the clear, deep, and dark web. Their family, social, and professional circles are also targeted, typically through scraping technologies such as social media avatars paired with bots that pivot from one data point to another to aggregate more information until all indexable data is exhausted. Once the data is compiled, a digital footprint is created and analyzed to identify vulnerabilities[6] and define the cyber exposure. The final step involves exploiting this attack surface through scenarios tailored to the individual's vulnerabilities (account impersonation, smishing, spear phishing, MFA bypassing, etc.), a form of "weaponization." The most critical step in this value chain is data collection.

Several examples illustrate the threat and its consequences, highlighting the human factor. In summer 2024, thousands of Ukrainian families were targeted by social engineering attacks, destabilization efforts, and banking fraud based on the names of Ukrainian soldiers identified on the Eastern front. Two years earlier, in February–March 2022, Russian troops were geolocated using dating apps like Tinder©. In fall 2023, a major defense industry player[7] suffered five months of data leaks via ransomware. While large defense groups invest in cybersecurity, their 4,000 subcontractors often lack the same resources and become targets of indirect attacks. In January 2024, an aerospace SME[8] discovered company computers infected with infostealers.[9] Later, several employees found their personal PCs also infected. A single personal computer exposed 200 login credentials, including professional ones.

In early 2025, the French president's movements were accurately anticipated[10] via the STRAVA© fitness app used by bodyguards. Two months later, again via STRAVA©, the layout and access points of the highly classified Île-Longue military base, home to nuclear missile submarines, were revealed. That echoed previous alerts raised during military use of the app in Iraq (2010), Afghanistan (2011), and Mali (2018), where operational base outlines had been inadvertently exposed. In July 2024, a test conducted in a French sovereign ministry revealed a critically high cyber exposure among its top twenty senior officials. The 2024 compromise of the *elysee.fr* email address of Emmanuel Moulin, Secretary General of the Élysée presidential palace, further confirms the threat reaches the highest levels of state. These cases highlight the counterintuitive fact that leaders are often the most cyber-vulnerable.

This is confirmed by another case: a woman from a CAC 40 company's executive committee, negotiating in Southeast Asia, received a call on her personal phone just an hour before a decisive meeting: "Are you the mother of Julien and Marie[11] who attend the *lycée* … in the 15th arrondissement in Paris? We're nearby." The caller hung up. After notifying the school and her husband, she continued with the negotiation, which ended in failure.

---

[5] This is a definition from Cyber Threat Intelligence (CTI) service of ANOZR WAY company. https://anozrway.com/fr/

[6] "In legislation and cybersecurity literature, there are three terms often used as synonyms, though they are in fact distinct: vulnerability, cyber threat, and risk. The greater the (digital) exposure, the higher the vulnerability; conversely, the greater the response capacity, the lower the vulnerability. This means that vulnerability = exposure / response capacity." — *Dr. Emilie Musso*

[7] The name of the company cannot be disclosed for reasons of confidentiality and protection.

[8] *Ibid* 5

[9] An infostealer is a term used in computing to refer to a type of malicious software designed to infiltrate information systems and steal sensitive data. This may include login credentials, financial information, or other personal data. Examples include: Redline**,** Vidar**,** RacoonStealer**,** Stealc**,** and Trojan**.**

[10] Members of the Presidential Security Group (GSPR) use their STRAVA© application to record — and sometimes even publish — their running performances while carrying out reconnaissance missions for the President's upcoming movements.

[11] The first names have been changed.

Cognitive and behavioral biases are essential keys to understanding

"The threat no longer enters through a technical flaw. It infiltrates minds, emotions, and daily habits. The human factor has become the main battlefield. And in this silent war, personal data is both ammunition and the prize. The attack begins with an Instagram photo, a LinkedIn contact list, or a jog posted on STRAVA. Every click, every share, every moment of naivety is exploited, recycled, and amplified. It's an invisible suffocation strategy: you're scraped, indexed, profiled, and then turned against yourself."

What cybersecurity still struggles to grasp, attackers have already mastered: they don't target systems, but decisions, cognitive vulnerabilities, and human reflexes. It's no longer about defending an information system, it's about reclaiming our own narratives, our exposure, our mental sovereignty. While companies build walls around their servers, it's a single personal phone call, a child's voice, a school question, a silence, that breaks through. This is how psychologist Nathalie Granier, an expert in cybersecurity, illustrates the behavioral and cognitive dimensions.[12]

Behavioral analysis examines user and attacker behavior to anticipate threats and strengthen security. In essence, it's a form of profiling.[13] This approach is vital to characterize threats and identify countermeasures. In this new battlefield, thought itself becomes a vector of intrusion.

According to Nathalie Granier, "Behavioral analysis addresses three main areas. First, analyzing the crime scene: in cyber, this means collecting digital forensic evidence like logs and connection times. Analysts then correlate these data points. Second, they gather forensic team documents. Finally, profiling involves analyzing attacker behavior and characteristics to create profiles that help identify them. This helps technical teams answer questions like: What did the adversary do? What are their objectives? Who are they? What will they do next? Ultimately, it helps detect threats, respond to incidents, and improve defense." Besides psychology, disciplines like geopolitics, linguistics, and sociology also play crucial roles.

Nathalie Granier also stresses the limitations of behavioral analysis: privacy concerns, cognitive biases, false positives, lack of data, and methodological constraints.

Legal insecurity around data rights undermines the defense continuum

Cyberspace is now a zone of conflict. States wage open cyberwar while criminal networks thrive. Alongside system attacks and mass data breaches, manipulation tactics flourish. These strategies echo the 2020 doctrine[14] of Russian General Gerasimov,[15] describing total information warfare, digital combat, indirect approaches, immaterial domains, and proxy warfare where creativity is encouraged at all levels to destabilize adversaries and force degraded responses.

[12] Statements collected during an interview, May 27, 2025.
[13] Profiling, according to the GDPR definition, "is the automated processing of personal data consisting of using such data to evaluate certain aspects of the data subject, and to analyze or predict their interests, behavior, and other attributes."
[14] Restricted access document. French ministry of defense sources.
[15] Valery Vassilievich Gerasimov is a General of the Army and has been the Chief of the General Staff of the Armed Forces of the Russian Federation since November 9, 2012. He is also the First Deputy Minister of Defense.

In this context, democratic rule-of-law states find themselves in asymmetric warfare, forced to fight with legal weapons. An unsolvable equation.

Legal voids remain around data rights, particularly for personal data on the dark web. This raises the question of how and why to legally secure data and its use across all internet layers to protect individuals and organizations exposed to targeted attacks. In France especially, the precautionary principle often results in self-censorship. But if the goal is to protect people and property or inform already-targeted individuals, is it really against the spirit of the law? Isn't such action justified by its purpose?

This question is being tackled by a working group supported by the IHEDN Chair for Cyber and Digital Sovereignty and the Alliance for Digital Trust, co-led by Prof. Michel Séjean[16] and Dr. Émilie Musso. Their goal is to develop legislation that, according to Musso,[17] "would not seek to restrict, but rather to empower and legally protect open-source intelligence practitioners and their subjects, eliminating the legal vacuum that paralyzes both public and private response to a rampant, uninhibited threat."

Counterintuitively, even France's privacy watchdog CNIL supports this initiative, highlighting in a recent report[18] the growing scale of data theft and the urgent need to reinforce all areas of cybersecurity. Moreover, recent European cybersecurity regulations require processing data from leaks to comply at least with the spirit of the law, even if it is not yet fully finalized. One delegated act complementing the DORA Regulation requires financial entities to detect data breaches;[19] DORA mandates processing open-source data for cybersecurity,[20] including cyberattack intelligence and monitoring[21] that use leaked data.[22] Similarly, the NIS 2 Directive mandates cybersecurity tools to detect cyberattacks,[23] including data breaches, thus justifying the processing of leaked data.

[16] Michel Séjean is a professor at Paris XIII University and an associate researcher at IHEDN, specializing in cybersecurity law and comparative law. He is also the scientific director of the Code de la cybersécurité published by Dalloz. He is supported in his work by numerous experts from the legal field (notably Dr. Émilie Musso — a French expert in digital data law), as well as professionals from various ministries and parliamentarians.

[17] *Ibid* 14

[18] In 2024, the CNIL was notified of 5,629 personal data breaches, representing a 20% increase compared to 2023. Beyond this notable rise, the most concerning trend is the surge in very large-scale breaches. In addition to unprecedented breaches affecting third-party payment operators, the French employment agency France Travail, and the telecom company Free, the CNIL observes that the number of violations impacting over one million people has doubled within a year. In response, the CNIL has made cybersecurity one of the four pillars of its 2025-2028 strategic plan. In practice, its actions include:

- Supporting organizations by issuing recommendations to protect personal data in light of evolving threats and state-of-the-art practices;
- Conducting audits to verify the implementation of security measures by organizations;
- Informing and raising awareness among individuals about cybersecurity to empower them in protecting their data.

[19] Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regulatory technical standards specifying the tools, methods, processes, and policies for managing ICT-related risks, and the simplified ICT risk management framework (RTS on ICT risk management framework), Article 14, point 1(b); Article 34(i).

[20] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011, recital 56; Article 25, point 1.

[21] *Ibid*., art. 10, 3°.

[22] *Ibid*., art. 3, 15°; art. 13, 1°.

[23] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), Article 29.

Toward a necessary structuring of the response in a security continuum[24]

Viewing cyberspace as a socio-technical construct invites us to look beyond technology and acknowledge its social and political dimensions, as it is ultimately a human product. It is misguided to believe that technical solutions alone can address the full scale of threats faced by organizations, businesses, or states in this new environment.[25] User behavior, particularly digital footprint and vulnerability, is crucial and must be considered. Cybersecurity analysis should thus systematically combine social, human, and technical approaches.

Cybersecurity is a strategic issue and should be addressed at the highest organizational level.[26] Managerial, operational, and technical perspectives must converge. Yet, a truly global approach[27] is lacking, even among CAC 40 companies,[28] Western military commands[29] and governments, despite the fact that cyber risk today merges digital and informational threats, with the human factor as the primary threat vector.

Paths to explore for a structured response might include strong executive sponsorship, cybersecurity cross-functionality, information sharing,[30] integration of digital, informational, and communication domains, comprehensive human factor considerations, and dual capabilities, to both protect and act within the cyber–digital–informational–cognitive continuum, thereby fostering a broader continuum of security.

Conclusion

Ultimately, as AI plays an increasingly significant role in the cyber domain, whether in attacks, data analysis, or protection, the human factor appears as both the problem and the solution.

---

[24] The concept of a continuum of security addressing human risks, cyber threats, and influence warfare was discussed and illustrated on May 20, 2025, by Anne Tricaud (Head of Security – Airbus), General (Ret.) Stéphane Dupont (Security Director of NavalGroup), Chloé Debièvre (specialist in influence and information warfare), and Émilie Bonnefoy (Open Sezam) during their appearance on the program *RiskIntelMedia*, hosted by Yasmine Douadi.

[25] Amaël Cattaruzza and Jérémy Buisson, *The Sociotechnical Dimension of Cyberspace, in Cybersecurity*, 2nd edition, 2023, Armand Colin.

[26] Like many aspects—such as organizational simplification or transformation processes—without strong sponsorship, the efforts required will be considerable for modest results.

[27] However, there are policies that lay the foundations for such structuring, as illustrated by the Security Plan (PSSI) and Continuous Security Improvement Plan (PACS) of France's national computer security agency. These two plans aim to structure the response around four pillars: governance, protection, defense, and resilience. Within governance, ANSSI addresses the management of the human factor (awareness and training), but informational and cognitive issues are overlooked.

[28] When analyzing the organization of cybersecurity within France's CAC 40 companies, the following roles are found at various levels of responsibility: Chief Information Officer (CIO), Chief Technology Officer (CTO), Chief Data Officer (CDO), Chief Security Officer (CSO), Chief Information Security Officer (CISO), and Data Protection Officer (DPO). While many dimensions are considered, the human factor and informational-communicational aspects remain largely absent.

[29] This segmentation in the private sector is also present within most Western militaries and NATO, where many functions still operate in silos, similar to the various roles within a joint staff: intelligence (J2), operations (J3), information and communication systems (J6), influence and environmental action (J9), along with operational communication (COM OPS), which generally reports directly to command, and cyber influence operations (L2I), which fall under the strategic level.

[30] At the Paris Cyber Summit held from June 3 to 5, 2024, the issue of information sharing was raised—both within a state and internationally, between the public and private sectors—in what could be described as "circles of trust." This information sharing, still insufficient, could be a first step toward breaking down silos. NIS 2 encourages EU member states to strengthen this sharing.

Indeed, individuals' cyber exposure and cognitive biases, combined with the cyber criminals' growing capabilities to capture, analyze and manipulate information, position the human factor as the central issue, both for those behind the threat and for those striving to defend against it.

In this context, the structuring of cyber defense has become a matter of vital interest.

References

Solange Ghernaouti, "Cybersecurity," 7th edition, DUNOD.

Amaël Cattaruzza and Jérémy Buisson, *The Sociotechnical Dimension of Cyberspace,* in "Cybersecurity," 2nd edition, 2023, Armand Colin.

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011, recital 56; Article 25, point 1.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), Article 29.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), Article 29.

Cybersecurity Code 2024 annotated and commented, *Preventing cyber risk, defending your activity and your intangible assets*, 10/2023 – DALLOZ, 2nd edition | Author(s): Michel Séjean, Marc Watin-Augouard, Brunessen Bertrand, Nicolas Catelan, Thibault Douville, Valère Ndior, Emmanuel Netter, Anne-Thida Norodom, Matthieu Audibert, Warren Azoulay, Thibaut Heckmann.

CNIL (2005), "Le bilan et les actions marquantes de la CNIL en 2024," pages 49-54. https://www.cnil.fr/sites/cnil/files/2025-04/rapport_annuel_2024.pdf

Risk Intel media, Yasmine Douadi, *Why the threat has no limits, decryption,* broadcast on the internet, May 20, 2025. https://www.youtube.com/watch?v=WsrOtvnxlWk&list=PL3tV-BWrLE3xsLLzbf0omsatELMln_EFR&index=4

Interviews with Dr. Émilie Musso, legal expert in data law, co-director of the working group of the Institut des Hautes Études de la Défense Nationale (IHEDN) on the law of open-source digital research, contributor to the cybersecurity code, and legal advisor to the company ANOZR WAY. In Rennes and Paris, April and May 2025.

Interview with Nathalie Granier, psychologist, expert in cybersecurity and behavioral analysis in response to cyber risks and attacks. In Paris, May 30, 2025.