

BULLE CYBERNÉTIQUE. VAPORIZING THE SCENT OF CYBER THREATS

Elena Abbiatici

Albertina Academy of Fine Arts of Turin
elena.abbiatici@gmail.com

ESSAY 170/12

CYBER WARS

ENIGMA CODE

TRADE AND MIGRATION ROUTES

VOLATILITY OF DATA

BACTERIAL POWER

Bulle Cybernétique is an artistic project conceived by Elena Giulia Abbiatici and developed with the professional nose Diletta Tonatto, that explores cybernetic warfare through olfactory language as both an aesthetic and political tool. It explores the use of the olfactory code as an unconventional means of communication capable of circumventing government restrictions and media censorship. Considering essences as a multidimensional medium, olfactory stimuli challenge traditional methods of information transmission,

assuming a crucial role in the processes of encoding and decoding messages. Through an interdisciplinary approach that interweaves art, cybersecurity and geopolitics, the paper analyses three key dimensions of the project: 1) the need for new communicative codes that, involving little-explored senses, overcome transnational barriers and digital surveillance; 2) the relationship between digital attacks and chemical-bacteriological strategies; 3) the impact of submarine network infrastructures on ecosystems.

INTRODUCTION

Contemporary wars are fought on multiple fronts, redefining the very concept of conflict and power. Cyberspace has become a strategic battleground, characterised by targeted attacks on critical infrastructures, information control and national security. In parallel, the manipulation of the environment through chemicals and biological agents remains a real threat, capable of altering living conditions and exerting invisible but pervasive forms of social control. Against this backdrop, *Bulle Cybernétique* introduces an innovative paradigm that explores olfactory language as a tool for transmitting and decoding information, transforming cyber-war data into an interpretable essence and raising questions about the materiality of the global network and its physical infrastructure.

Air, a ubiquitous and indispensable medium, is now at the centre of a complex web of ecological, political and technological issues. The concept of *atmoterrorism* (Sloterdijk, 2009)- i.e. the pervasiveness of particulate matter, nitrogen oxides, carbon monoxide and other suspended pollutants - reflects an insidious form of environmental and health aggression that affects human life in a deceptive and constant manner. As Peter Sloterdijk suggests, the beginning of the modern era can be traced back to the use of tear gas and blister agents during the First World War –including chlorine, phosgene, and mustard gas– followed by Zyklon B in the Nazi concentration camps, the deployment of sarin and chlorine gas in Syria during the 2010s, and more recently the growing concerns around genetic manipulation and the potential production of advanced biological weapons. These examples demonstrate how the biochemical dimension of warfare remains an unresolved and ever-present field of tension: suffice it to recall that as early as 1763, during the war for control of North America, the British army distributed blankets contaminated with smallpox to the Ottawa people, employing them as a bacteriological weapon.

Bulle Cybernétique thus proposes a critical reflection on the gaseous dimension of power. The sense of smell and breath, understood as measurable and manipulable biochemical data, are in fact part of the dynamics of bio-surveillance, delineating new forms of interaction between body, technology and environment. The recent Covid-19 pandemic has made the centrality of air and breath in global crisis dynamics even more evident, prompting a critical reassessment of the relationship between bioattacks, biopolitics and sensory perception. The enemy is no longer only physical, but increasingly aerial.

In this context, the project questions the role of olfactory design not only in the purification and conditioning of air –factors that contribute to environmental and economic inequalities– but also in its capitalisation and potential use as a tool of power and control. The attempt to decode the invisible is a topic that is particularly close to the most current reality: the invisible is found between the lines of information, in memory databases, in biometric controls, and manifests itself in a virus, encrypted information, a biometric parameter or an act of cyber warfare.

CONCEPT OVERVIEW

Bulle Cybernétique (BC) is the first gesture of a speculative research that embodies the perturbing aspects of technology, unveiling underground and invisible facts through a mysterious, seductive, aerial, and ephemeral essence. Specifically, *Bulle Cybernétique* is a scented essence designed as an *enigma code*, a cipher code, to hypothetically communicate and decrypt successful, foiled, or still fearsome cyber attacks and reflect cyberwarfare through the aromatic volatility of data. The submarine wired network –dominated by content providers, social media and private companies– shape the current *Undersea Continuous Monument* by Superstudio (fig. 1): one of the most influential and polluted places in the world.

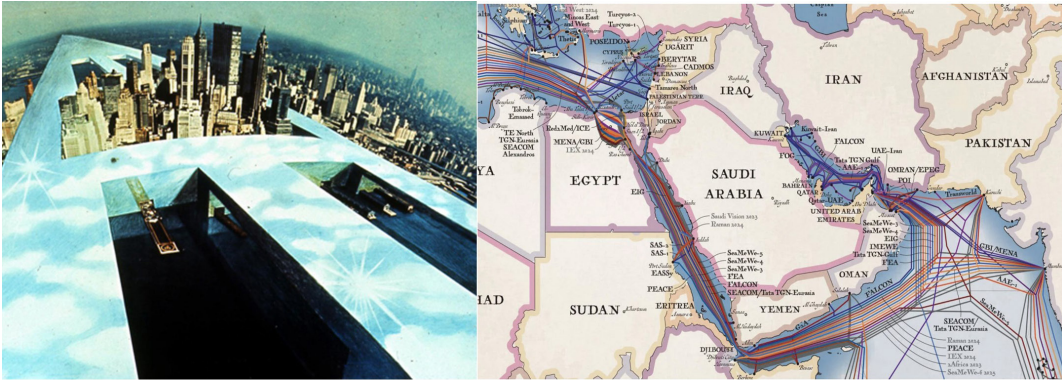


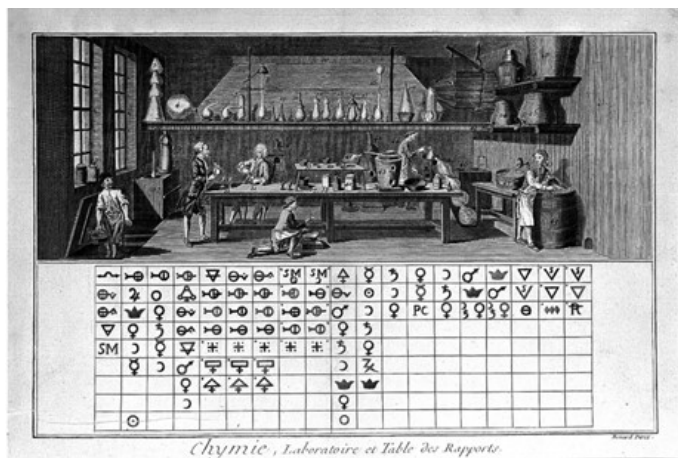
Fig. 1 On the left: Superstudio, *The Continuous Monument*, 1970; on the right: Subsea cables traversing the Red Sea seabed (Source Middle East Eye).

Bulle Cybernétique is a luxury product potentially able, as a marketable product, to avoid state confinement measures and information control, while containing encrypted data. Unlike people crossing sea and land, flow of data and capital in movement are not interrupted. *Bulle Cybernétique* is thus a hypothetical artistic form of secret communication that, by engaging with the transnationality of air, reveals the potential bio-chemical threats constantly present in the atmosphere, which indeed remains largely unconfined.

Practically, the scent formula has been developed by analyzing World Cyber Crime Index and three major cyber incursions involving countries and large companies. Each type of attack, as well as the States or companies involved, is associated with specific olfactory notes based on precise associative criteria, which the code has been instructed with. The code is designed to inform the essences with salient components of cyber offensives (offending or affected countries, type of threats, impacts, risks), in order to translate them into a geopolitical and eco-systemic chronicle.

The development of a code that can facilitate the creation and decoding has been conceived in collaboration with Diletta Tonatto –a fine nose and sociologist of olfaction, and founder of Tonatto Profumi, one of the most prestigious Italian perfume houses– and with the Cybersecurity Expert, Eng. Eridia Bozzetti. The focus has been placed on essences of a bacterial nature in order to dwell

Fig. 2 Laboratory and Table of Affinities. Engraving from *Recueil des planches sur les sciences, les arts libéraux, et les arts mécaniques*, vol. 2, Paris, 1768 (entry “Chimie”), illustrating an 18th-century chemical laboratory and an affinity table. Public domain.



on the ambivalence reserved for the microcosm of viruses and bacteria (fig. 2). In an era where spaces tend to be increasingly sterilized and devoid of character, the intention is to exorcise the anesthetization of environments, creating fragrances capable of redefining sensory and cultural codes of smell, challenging the social construction of the concepts of ‘good’ and ‘bad’ odors. The use of bacteria fermentation in the production of essences offers several advantages: sustainability –avoiding deforestation and the intensive exploitation of plants; olfactory consistency– the essences obtained through fermentation are more stable and free from the typical variations of natural extracts; innovation –it allows for the creation of new molecules or the enhancement of existing ones, expanding the olfactory palette for perfumers. Therefore, the fragrance would be decrypted either through the fine experience of professional noses and analytical chemists by using a technique called *headspace analysis* in combination with *gas chromatography*, to determine the chemical components of the essences formula and read the ‘encrypted message’ they carry. Headspace analysis plays a crucial role in identifying volatile compounds in the gaseous part of the fragrance. Gas chromatography facilitates the separation and analysis of these components, enabling a precise formulation of the essence.

Bulle Cybernétique seeks to embody the unsettling nature of technology –both geopolitically and environmentally– while rethinking the relationship between digital and bio-chemical codes, transforming it into a multidimensional tool for understanding digital threats. As Arthur C. Clarke famously stated.

METHODOLOGY BEHIND THE OLFATORY CODE

Mapping the global geography of cybercrime

The study adopted an interdisciplinary approach, integrating both quantitative and qualitative analyses of cyber threats, with a sensory translation of the data through olfactory design.

To situate the research within existing knowledge, a first step was the examination of global mappings of cybercriminal activities. This included consulting geopolitical publications and cybersecurity treaties, as well as real-time cyber-attack maps. Two key references guided this phase: the *World Cybercrime Index* (Bruce et al., 2024), which identifies the principal actors and countries most active in cybercrime, and the *ENISA Threat Landscape 2023*, the annual report of the European Union Agency for Cybersecurity (figg. 3-5). Together, these sources provide both a geopolitical overview and a typological classification of threats. The ENISA report, in particular, outlines the most relevant forms of attack (Ransomware, Malware, Social Engineering, Data Breaches, Denial of Service, Web Threats, Supply Chain Attacks, and Foreign Information Manipulation and Interference) while also assessing their impacts across economic, military, social, reputational, physical, political, and environmental domains.

Building on these mappings, the research isolated the 97 countries most involved in cybercriminal activities, either as perpetrators or as targets. From this dataset, the project developed its own methodological

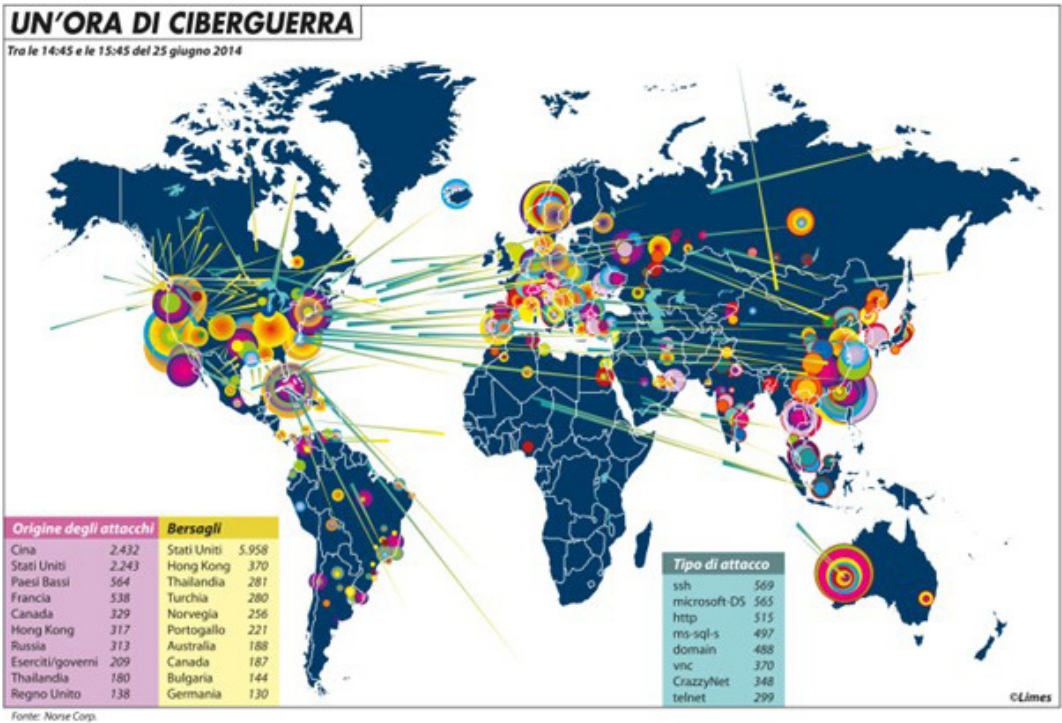


Fig. 3 Map designed by Laura Canali for Limes, Italian geopolitical magazine. (It should be understood as an evocative reference, rather than a direct source of data).

contribution: a sensory translation of threat typologies and their impacts through olfactory design. In this way, the study does not simply replicate existing cartographies but extends them into an embodied, experiential dimension that reveals the often intangible nature of digital offensives.

Three emblematic case studies of cyber attacks were selected on the basis of their geopolitical relevance, technological sophistication and multiple impacts: the Stuxnet malware, the NotPetya ransomware and the Office of Personnel Management (OPM) data breach. Each type of attack was analysed in terms of actors involved, risk vectors and strategic consequences. This information was then associated with specific olfactory notes through the writing of a code, so as to create a correlation between the characteristics of the attack and the selected essences. The resulting olfactory code

Rank	Country	I	P	TS	WCI Score	Tech	Attacks	Data	Scams	Cash
1	Russia	8.96	8.81	8.73	58.39	82.17	81.34	65.18	21.70	41.56
2	Ukraine	8.37	8.29	8.24	36.44	52.97	50.76	36.01	11.20	31.27
3	China	8.22	7.70	7.81	27.86	40.22	24.24	34.89	15.83	24.13
4	United States	7.99	7.21	7.21	25.01	27.64	17.68	30.36	22.72	26.63
5	Nigeria	8.25	6.49	5.80	21.28	7.93	8.41	23.04	52.17	14.86
6	Romania	7.12	7.04	7.15	14.83	17.83	9.17	22.50	13.15	11.49
7	North Korea	7.91	7.23	7.38	10.61	8.66	25.33	13.01	2.17	3.88
8	United Kingdom	7.86	7.21	6.75	9.01	5.04	4.75	5.80	7.86	21.63
9	Brazil	6.90	6.35	6.32	8.93	13.70	8.77	10.29	7.28	4.64
10	India	7.90	6.60	6.65	6.13	4.46	3.62	6.81	12.75	3.01
11	Iran	6.88	6.45	6.64	4.78	8.62	10.00	3.59	0.94	0.72
12	Belarus	6.84	7.20	7.32	3.87	11.92	5.58	1.85	--	--
13	Ghana	8.57	6.83	6.09	3.58	1.23	0.76	2.97	10.36	2.57
14	South Africa	6.95	5.35	5.50	2.58	1.20	0.65	0.58	7.17	3.30
15	Moldova	7.38	7.19	7.56	2.57	6.70	0.98	2.43	0.83	1.88

I = Impact; P = Professionalism; TS = Technical skill, Technical = Technical products/services, Attacks = Attacks and extortion, Data = Data/identity theft, Cash = Cashing out and money laundering. I, P, and TS are scored out of 10. 'WCI Score', and all columns following, are scored out of 100. Each country's top score across all cybercrime types is shaded in grey.

Fig. 4 From: Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). *Mapping the global geography of cybercrime with the World Cybercrime Index*. PLOS ONE, 19(4), e0297312. <https://doi.org/10.1371/journal.pone.0297312>

was then tested and validated by means of professional noses and headspace analysis in combination with gas chromatography techniques, which made it possible to isolate and identify the volatile compounds responsible for the final scent.

Diagram

The olfactory triangle used to map cyber warfare follows the structure of traditional perfumery pyramids (fig. 6), where top notes represent the most volatile and immediately perceptible elements, heart notes emerge gradually over time, and base notes linger the longest, leaving a lasting impression.

In this model, the first elements to surface are the targeted countries (X) and the nature of the risk (W), both embodied in the top notes. The affected nations are represented by fresh, herbaceous essences, while the risk level is conveyed through balsamic notes, distinguished by two intensities: basil for medium risk and eucalyptus for high risk.

Next, the heart notes unveil the type of cyber intrusion (Y1) and its impact (Y2). The different forms of cyber threats are distinguished through subtle floral hints: eight flower essences representing eight attack categories (Ransomware, Malware, Social engineering, Data breach, DDos atmoterrorism –Denial of Service, Web Threats, Supply Chain Attacks,

This table represents the list of olfactory notes associated to countries involved in cyber attacks as attacker or attacked

LIST OF COUNTRIES (1-49)

LIST OF COUNTRIES (50-97)

Table S1. World Cybercrime Index - Overall

X	Rank	Name	Country	I	P	TS	Overall	WCI Score	Z
Landmark	1	301	Thailand	6.56	8.51	8.36	7.81	54	Amber
	2	302	Ukraine	6.57	8.29	8.36	7.81	54	Amber
	3	303	China	6.52	7.79	7.81	7.50	27.86	White musk
	4	304	United States	6.50	7.25	7.81	7.50	25.01	Vanilla
	5	305	Nigeria	6.25	6.49	5.80	6.50	21.28	Vanilla
	6	306	Romania	7.12	7.26	7.25	7.27	14.83	Vanilla
	7	307	North Korea	7.91	7.23	7.28	7.51	10.61	Vanilla
	8	308	United Kingdom	7.96	6.50	6.51	7.27	9.01	Vanilla
	9	309	Brazil	6.90	6.50	6.52	6.52	8.93	Vanilla
	10	310	India	6.99	6.45	6.44	6.48	4.78	Vanilla
Field Grain	11	311	Belarus	6.54	7.29	7.32	7.12	3.87	Vanilla
	12	312	China	6.57	6.43	6.09	7.18	3.58	Vanilla
	13	313	South Africa	6.55	5.25	5.50	5.50	2.59	Vanilla
	14	314	Maldives	7.28	7.19	7.06	7.28	2.17	Vanilla
	15	315	Israel	6.43	6.22	6.27	6.29	2.12	Vanilla
	16	316	Poland	6.46	7.92	7.15	7.65	2.12	Vanilla
	17	317	Germany	6.00	7.54	7.54	7.08	2.12	Vanilla
	18	318	Netherlands	7.75	7.25	7.08	7.28	1.92	Vanilla
	19	319	Latvia	6.73	7.26	7.08	7.08	1.89	Vanilla
	20	320	Kazakhstan	7.09	6.51	7.00	7.00	1.67	Vanilla
Field Grain	21	321	Vietnam	7.08	5.92	5.53	6.11	1.59	Vanilla
	22	322	Estonia	6.90	7.00	7.00	7.00	1.59	Vanilla
	23	323	United Arab Emirates	7.09	6.79	6.90	7.13	1.55	Vanilla
	24	324	Canada	6.90	7.08	7.75	7.75	1.34	Vanilla
	25	325	Malaysia	6.53	6.59	6.53	6.58	1.33	Vanilla
	26	326	Philippines	6.27	5.90	6.27	5.98	1.24	Vanilla
	27	327	Peru	5.50	5.79	5.80	5.80	1.22	Vanilla
	28	328	France	6.40	6.40	7.08	6.71	1.17	Vanilla
	29	329	Indonesia	6.48	6.48	6.38	6.71	1.17	Vanilla
	30	330	Belgium	6.62	6.48	6.08	6.17	1.07	Vanilla
Field Grain	31	331	Thailand	7.43	6.57	5.71	6.57	1.00	Vanilla
	32	332	Mexico	7.14	6.14	6.08	6.40	0.98	Vanilla
	33	333	Australia	6.50	5.98	4.98	5.48	0.95	Vanilla
	34	334	Italy	7.40	7.40	7.40	7.40	0.95	Vanilla
	35	335	South Korea	7.40	7.40	7.40	7.27	0.79	Vanilla
	36	336	Guatemala	6.50	5.40	5.40	5.47	0.79	Vanilla
	37	337	Columbia	7.20	6.60	5.60	6.47	0.79	Vanilla
	38	338	Ghana	6.50	6.00	6.00	7.17	0.82	Vanilla
	39	339	Czech Republic	6.90	7.25	5.60	6.71	0.59	Vanilla
	40	340	Netherlands	6.75	6.75	5.75	6.30	0.51	Vanilla
Field Grain	41	341	Cyprus	6.33	7.67	6.00	6.90	0.52	Vanilla
	42	342	Cyprus	6.67	6.60	5.40	7.09	0.51	Vanilla
	43	343	Maldives	6.75	5.25	5.50	5.43	0.51	Vanilla
	44	344	Palau	6.75	4.90	4.50	5.75	0.50	Vanilla
	45	345	Kenya	6.75	4.90	4.50	5.75	0.50	Vanilla
	46	346	Lebanon	6.75	4.90	4.50	5.75	0.50	Vanilla
	47	347	Lebanon	6.67	6.67	6.67	7.25	0.49	Vanilla
	48	348	Maldives	6.75	4.75	4.50	5.17	0.45	Vanilla
	49	349	Phnom	7.08	7.25	6.25	6.98	0.45	Vanilla

January 9, 2024

1/25

* <https://doi.org/10.1371/journal.pone.0297312>

Fig. 5 Full indices for the World Cybercrime Index Overall and each WCI Type.
<https://doi.org/10.1371/journal.pone.0297312>

FIMI– Foreign Information Manipulation and Interference). The consequences of the intrusion, on the other hand, are conveyed through fruity notes symbolizing its economic, military, social, reputational, physical, political, or environmental ramifications.

Finally, the base notes, the last to fade yet the most enduring, correspond to the identity of the attackers (Z), expressed through woody, musky, and amber essences, embodying the origins of the cybercriminal act. The distinctiveness of each resulting fragrance mirrors the uniqueness of digital signatures.

THREE EXEMPLARY ATTACKS

Stuxnet: the cyber attack that shook the nuclear infrastructure

The Stuxnet attack (2010) is considered one of the most sophisticated and innovative cyberattacks in history. It has been widely attributed to a collaboration between the

This diagram represents the code message used by the cyberattacker countries to send secret information

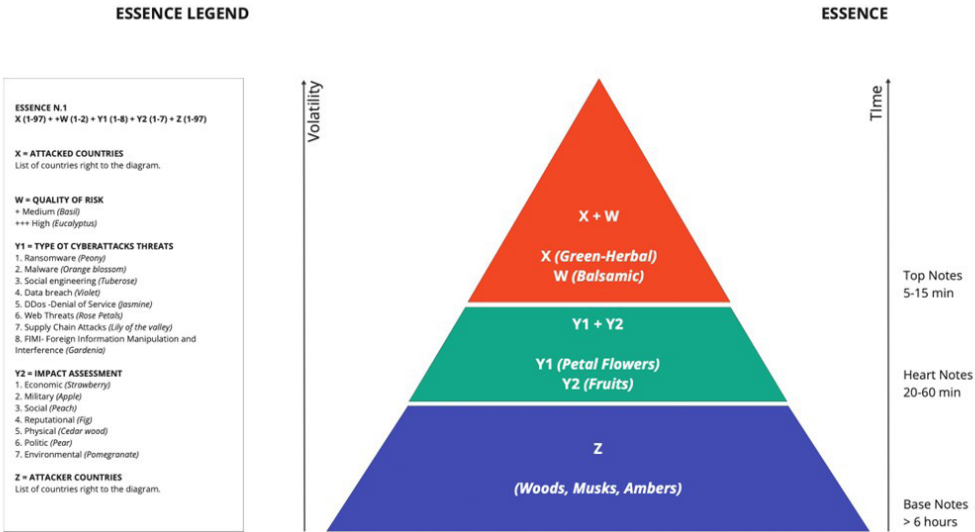


Fig. 6 Diagram illustrating an olfactory coding scheme used to encode the components of a cyber attack. The figure combines an essence legend with a structured olfactory pyramid (top, heart, and base notes), mapping geopolitical actors to scent-based attributes, risk level, threat types and impact categories. The pyramid maps top notes (target country and risk level), heart notes (attack types and impact categories), and base notes (attacker country), illustrating the temporal persistence and qualitative attributes of the encoded elements.

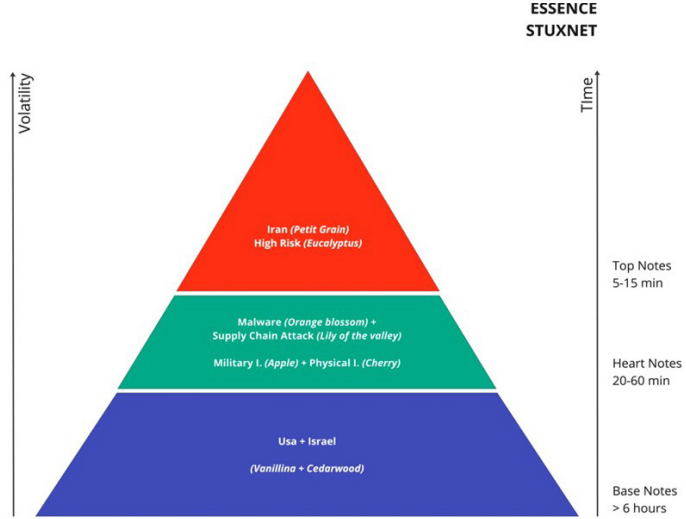
United States and Israel, although neither country has ever officially confirmed the operation. Designed specifically to target physical infrastructure, Stuxnet aimed to disrupt Iran's nuclear development, particularly the uranium enrichment facility in Natanz.

This malware-based attack spread via infected USB flash drives that, once inserted into the Supervisory Control and Data Acquisition (SCADA) system, exploited vulnerabilities in Siemens software, which controlled the centrifuges. The malware sabotaged the machines by manipulating their rotational speed, causing malfunctions and, ultimately, their destruction.

The impact of Stuxnet was primarily military, with direct physical repercussions on Iran's nuclear program. By deliberately slowing down Iran's nuclear capabilities, the attack reduced the country's ability to produce weapons-grade nuclear material. Stuxnet was not just a cyberattack—it caused real-world damage, leading to centrifuge failures through covert digital interference.

In the olfactory code, Stuxnet would manifest as an initial petit grain essence, followed by balsamic eucalyptus notes (representing the high level of risk). The heart of the

Fig. 7 Olfactory encoding of the Stuxnet cyberattack represented through a three-tier pyramid of top, heart, and base notes.

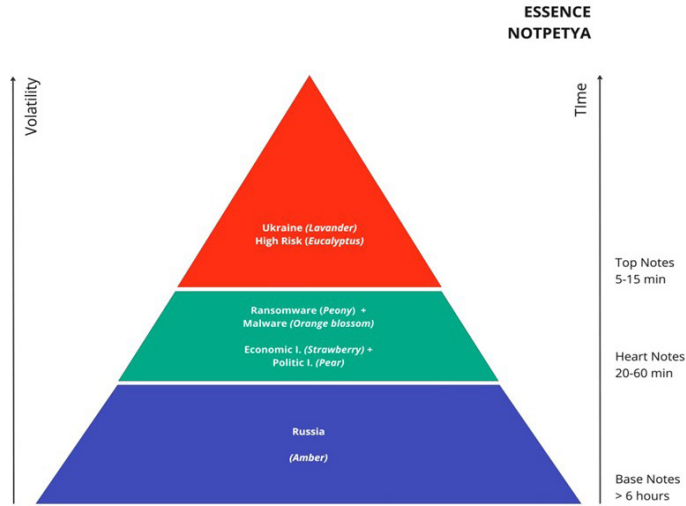


fragrance would feature orange blossom and lily of the valley (signifying the malware and supply chain attack), while apple and cherry notes symbolize its military impact and disruption of physical infrastructure. The attacking nations are represented by persistent base notes of Cedarwood (Israel) and Vanillin (USA) –olfactory markers that remain perceptible over time, mirroring the lasting geopolitical implications of the attack.

NotPetya: The Ransomware That Paralyzed the Global Economy

NotPetya, which struck on June 27, 2017, is considered one of the most devastating cyberattacks in history and is primarily classified as a ransomware attack. Although similar to Petya ransomware –which encrypts victims’ data and demands a ransom for decryption– NotPetya’s true purpose was far more destructive: to irreversibly wipe data, making recovery impossible even if the ransom was paid. The malware exploited EternalBlue, a Microsoft vulnerability originally developed by the National Security Agency (NSA) and later leaked by a hacker group known as Shadow Brokers. By leveraging a flaw in Windows systems, NotPetya enabled remote code execution

Fig. 8 Olfactory encoding of the NotPetya cyberattack represented through a three-tier pyramid of top, heart, and base notes.



without user interaction, allowing it to spread rapidly across corporate networks and infect interconnected systems.

The attack is widely attributed to a hacker group allegedly affiliated with the Russian government, though Russia has denied any involvement. Many experts, however, point to Ukraine as the primary target. In Ukraine, NotPetya crippled much of the country's digital infrastructure, affecting government agencies, banks, airports, public offices, and energy networks. Countries such as Germany, France, the United Kingdom, and other European nations reported significant disruptions. Among the hardest-hit multinational corporations were: Merck (U.S.), a leading pharmaceutical company; Maersk (Denmark), a global shipping and logistics giant; FedEx (U.S.), a major international transport company. The economic impact was catastrophic, with global losses estimated between \$10 and \$12 billion.

In the olfactory code, NotPetya's primary target, Ukraine, is represented by initial lavender notes, complemented by eucalyptus, which signifies the high-risk level of the attack. The heart of the fragrance is defined by peony essence, associated with ransomware, and orange blossom, symbolizing malware. These are enriched with fruity accents

of strawberry and pear, reflecting the attack's economic and political repercussions. As in forensic investigations, the presumed attacker –Russia– emerges only in the base notes, represented by amber, embodying its persistent and underlying influence on the event.

OPM Data Breach: The Cyberattack That Shook the United States

One of the most significant attacks in terms of national security was the Office of Personnel Management (OPM) Data Breach, which occurred in 2015. Hackers infiltrated OPM databases, stealing extremely sensitive data on approximately 21.5 million U.S. federal employees, including background check records, personal information (names, addresses, Social Security numbers), and even fingerprints. The attack was attributed to groups linked to the Chinese government and had severe consequences, putting U.S. national security and intelligence operations at risk. The data breach caused major reputational and political damage, seriously undermining the credibility of the U.S. government and raising concerns about its ability to safeguard sensitive employee data. The incident escalated tensions between the United States and China, fueling diplomatic and cybersecurity conflicts. Beyond its political ramifications, the attack had an inevitable social impact. The personal data of approximately 22 million people was exposed, leaving them vulnerable to identity theft, blackmail, and other forms of manipulation –a particularly alarming risk for those working in high-security government positions.

In the olfactory code, the attack initially emerges with a fresh green note of cut grass (USA), followed by basil, signifying, all things considered, a moderate risk level.

The heart of the fragrance is characterized by violet, representing the data breach typology, accompanied by fig, pear, and peach notes, which respectively symbolize the reputational, political, and social impact of the attack.

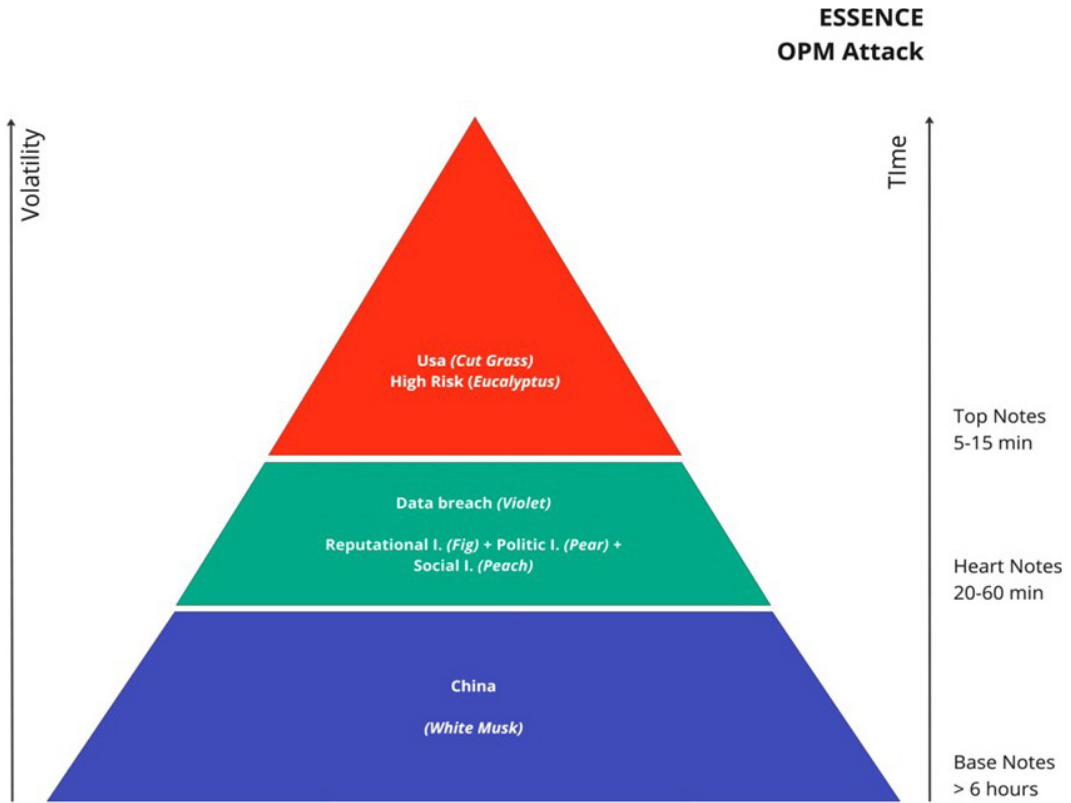


Fig. 9 Olfactory encoding of the OPM Attack represented through a three-tier pyramid of top, heart, and base notes.

Bulle Cybernétique is designed to train the nose, evoke emotions, and provoke thought, reflecting the complex interplay between digital language and the evocative power of scent. More than just a product, it is an immersive aesthetic experience that explores odours as a means of encryption and secret communication. While certain attacks and impacts are associated with specific essences (figg. 7-9), this translation is not intended as a simplistic one-to-one mapping. Rather, it is a deliberate strategy to render the code legible, opening the way for more nuanced interpretations in which fragrance becomes a layered medium—at once aesthetic, sensory, and political.

Research Framework and Key Themes

Olfactory data offers a unique form of communication,

often overlooked by conventional methods. While information can be blocked or censored, airborne substances such as scents are difficult to filter out, creating a paradox that BC explores. Despite the volatility to which both scent essences and digital data are subjected, scents can bypass censorship and governmental restrictions, communicating silently yet powerfully and providing a nuanced form of dissent.

This research seeks to rethink the transterritorial nature of geographical boundaries by examining how an essence vaporizes and carries its molecular compounds through the air, sparking a reflection on the political potential embedded in the atmosphere's metabolism. The study is driven by several key objectives, including rethinking the relationship between bio-chemical and digital codes and analyzing the environmental and financial consequences of data extraction.

THE IMPACT OF THE SUBMARINE CABLE NETWORK ON THE MARITIME ECOSYSTEM

The concept of the *continuous monument*, introduced in the 1960s by the avant-garde architecture and design collective Superstudio, can today be reinterpreted within the marine subsoil through the vast network of submarine Internet cables. This underwater infrastructure establishes an invisible grid that interconnects the world, though not without enacting a profound technological intrusion into the oceans. The Internet, in this sense, inhabits the seas, circulates through them, and facilitates the exchange between peoples and nations. It assumes the qualities of seawater—blue in color, infused with a phytoplankton-like scent, and imbued with a saline taste. Approximately 95% of global Internet traffic is transmitted via submarine cables, a system that is both indispensable and inherently fragile (Sherman, 2021).

The first public initiative of *Bulle Cybernetiqué* took place

in Malta during the symposium *Figure it Out: The Art of Living through System Failures* (September 18–20, 2024, Malta Society of Arts, Valletta). This project, co-funded by the European Union's Creative Europe program, investigates strategies of *sub-surveillance* in relation to technology and climate, with the aim of countering systemic exclusions frequently resulting from necessity or restricted access to essential services.

By situating its presentation in Malta, *Bulle Cybernétique* positioned itself at the very center of the Mediterranean—a region traversed by a dense network of submarine cables that connect Europe, Africa, and Asia. According to the European Institute of the Mediterranean (IEMED), up to 95% of trans-regional communication relies on these infrastructures. Such figures underscore the strategic centrality of the Mediterranean and its submarine routes in sustaining global connectivity.

However, the rapid expansion of this submarine infrastructure has profound environmental consequences. Cables laid along the ocean floor can damage fragile marine habitats, disrupt ecosystems, and interfere with the navigation and migration of marine species. Yet the impact is not confined to the sea. The digital infrastructure as a whole—submarine cables, data centers, and satellite networks—also has a measurable cost in the atmosphere. The extraction of rare earth minerals needed for the production and maintenance of these systems entails deforestation, air pollution, and greenhouse gas emissions, linking the seabed directly to the quality of the air we breathe.

The environmental cost of connectivity continues with the circulation and storage of data in the so-called “cloud,” whose physical manifestation requires vast energy resources. Data centers alone consume nearly 1% of the world's electricity and are responsible for approximately 0.6% of global CO₂ emissions, a figure projected to grow with ongoing digitalization (IEA, 2023). Every click, stream, or transfer of information thus generates an atmospheric trace, reminding us that immaterial flows are sustained by highly material, carbon-intensive infrastructures.

This convergence of marine disruption and atmospheric pollution raises urgent ethical and ecological questions: to what extent can the relentless pursuit of global connectivity justify the transformation of both oceans and skies? In an accelerating cycle of technological dependence, the submarine cable network becomes a material expression of what Max Weber termed the 'iron cage'—an economic and technological system advancing inexorably, driven by invisible data flows yet producing visible ecological costs.

CONCLUSION

Subjectively variable, immersive, spatially dissipated, olfactory spaces allow us to challenge the concept of *form*, shaped by an oculocentric perspective, and to look at the political and ecological sublimation of *matter* and its transcendence.

Bulle Cybernétique proves a lens to open up an ecological and digital problem, and allows us, through artistic research, to investigate the transnational condition of the atmosphere and its bio-political and aesthetic permeability on living organisms.

Besides being an olfactory experiment, *Bulle Cybernétique* is a critical reflection on the dematerialisation of conflict in the digital age, on the invisible infrastructures that sustain technological power, and on the transformation of the air into a sensory archive of data. Through the fading of the scent, the work invites the audience to question what remains after a cyberattack: traces that are imperceptible, but have concrete effects.

At the time of *atmoterrorism*, the nose fully regains its ancestral function as guardian and custodian.

REFERENCES

Sherman, J. (2021). *Cyber defense across the ocean floor: The geopolitics of submarine cable security*. Atlantic Council. <https://www.atlanticcouncil.org>

org/in-depth-research-reports/report/cyber-defense-across-the-ocean-floor-the-geopolitics-of-submarine-cable-security/
Sloterdijk, P. (2009). *Terror from the Air* (A. Patton & S. Corcoran, Trans.). Los Angeles: Semiotext(e) / MIT Press. (Original work published 2002 as *Luftbeben*, Frankfurt: Suhrkamp). ISBN 978-1-58435-072-9

ADDITIONAL READINGS

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024, April 10). *Mapping the global geography of cybercrime with the World Cybercrime Index*.
ENISA - European Union Agency for Cybersecurity. (2023, October). *Threat landscape 2023*.
International Energy Agency. (2023). *Data centres and data transmission networks* https://www.iea.org/energy-system/buildings/data-centres-and-data-transmission-networks?utm_source=chatgpt.com
IEMed. (2023). *The Mediterranean subsea: Protecting a super data highway*. European Institute of the Mediterranean. <https://www.iemed.org/publication/the-mediterranean-subsea-protecting-a-super-data-highway/>

Article available at

DOI: 10.60923/issn.2724-2463/21508

How to cite

Abbiatici E. (2025). BULLE CYBERNÉTIQUE. Vaporizing The Scent of Cyber Threats. *img journal*, 12, XXX-XXX.



© 2025 The authors. The text of this work is licensed under a Creative Commons Attribution 4.0 International License.