CYBERTALKS 2025

OUTUBRO 2025

EURODEFENSE-PORTUGAL

Palácio Bensaúde – Estrada da Luz, 151 - 1600-153 Lisboa

Preface

We live in a time when the boundaries between physical security, digital security, and geopolitical stability have become increasingly blurred. Technological globalization, combined with our increasing reliance on information networks, digital connectivity, and cybersecurity, has unlocked extraordinary opportunities while simultaneously introducing complex risks that threaten state sovereignty and societal resilience.

Given the importance of this issue in the context of European security and defense, **EuroDefense Portugal** decided to organize a cycle of ***CyberTalks***, aimed at fostering reflection, knowledge sharing, and multidisciplinary debate among academics, military personnel, policymakers, and representatives of the private sector. This publication is the result of that collective effort and seeks to continue the dialogue initiated in those sessions, offering readers a selection of particularly relevant contributions.

This volume brings together three highly topical texts that, taken together, provide a comprehensive view of the strategic challenges of the digital era, analyzing Portugal's geostrategic position within the global submarine cable system, the evolution of hybrid threats in the cyber domain, and the dynamics of recent conflicts in Ukraine and Gaza.

The first article, by Captain (N) Ret. Helder Fialho Jesus, provides a concrete analysis of the cyber dimension in two contemporary theaters of conflict: the war in Ukraine and the war in Gaza. Through these case studies, it becomes evident that cyberspace has evolved from a peripheral domain to a decisive front in the strategy of belligerents. In the Ukrainian case, cyber resilience was only possible thanks to the support of international allies and, in a groundbreaking way, private technology giants such as Amazon, Microsoft, Google, and Starlink. In Gaza, by contrast, one can observe the growing use of cyber operations by both state and non-state actors, particularly Iran, as well as the controversial deployment of artificial intelligence as a force multiplier—raising serious ethical and strategic questions.

The second article, authored by Colonel Luís Bernardino, highlights Portugal's role as a pivotal point in the worldwide submarine cable network. This system constitutes the true backbone of cyberspace, carrying the vast majority of global data traffic. By noting that Portugal is the only country directly connected by cable to all continents (with the exception of Antarctica), the author underlines not only the uniqueness of the country's geographical position but also the added responsibility to protect and enhance this strategic asset. Between opportunities for investment in smart cables and data centers, and vulnerabilities caused by the concentration of landing points, Portugal faces a dilemma between risk and potential that requires political vision, international cooperation, and long-term planning.

The third contribution, by Dr. Josef Schroefl, explores the concept of hybrid threats, with particular emphasis on the multiplier effect of cyberspace. The description of the three stages of a hybrid campaign—preparation, destabilization, and escalation to violence—demonstrates how disinformation, cyberattacks against critical infrastructure, and the use of proxies can weaken democracies without the need for direct military confrontation. The author warns that the "power of the weak," amplified by cyberspace, allows both state and non-state actors to project power with relatively limited resources. This framework makes it clear that defense against hybrid threats cannot be confined to government action alone: it requires a whole-of-state and whole-of-society approach, engaging citizens, businesses, academia, and multilateral institutions alike.

By bringing these three texts together, this publication provides an integrated vision of the intersection between geostrategy, cybersecurity, and hybrid threats. Portugal emerges as a central piece in this debate, not only because of its role as a global connectivity hub but also because of the urgent need to prepare for scenarios in which submarine cables, data networks, and digital systems become both targets and instruments of pressure. The reflections presented point in the same direction: It is imperative to strengthen collaboration among governments, international bodies, and private enterprises; to prioritize investments in technological robustness; and to foster a society that is informed and prepared to navigate the intricacies of the digital age.

This volume thus aims to contribute to an informed and necessary debate, bringing together different academic and professional perspectives on cyberspace security and its geostrategic impacts. It is now up to the reader, through these pages, to reflect on the challenges that lie ahead and on the role that Portugal and Europe can play in building a safer, more stable, and more cooperative cyberspace.

Eurodefense, Portugal

The dynamics of conflicts in Cyberspace

Captain (N) Helder Fialho Jesus (Retired)
Jesus.hmf@ium.pt

1. Introduction

The intention of this document is to provide a reflection of the actual wars in Ukraine and Gaza, focusing on cyberspace. This paper includes actors, provides support, and details events. Given the longer duration and distinct interests of the Ukraine war compared to the Gaza war, this paper focuses more on the former.

2. Ukraine

With the annexation of Crimea in 2014, the Russia-Ukraine conflict has been a significant political issue, with consequences in cyberspace. Since then, the US has been playing a significant role in Ukraine's foreign policy, supporting several significant reforms there and influencing international institutions, among them the North Atlantic Treaty Organization (NATO) and the International Monetary Fund (IMF). In 2017, a US-Ukraine bilateral cyber dialogue was established to strengthen national response planning, infrastructure security and information sharing, linking Ukraine with the US Defense, Energy, and Treasury departments. In the years prior to the Russian invasion in February 2022, Ukraine has participated in multinational exercises in cyberspace with NATO and other NATO allies.

To understand the conflict in the cyberspace domain, the “UNICEF Guide to Conflict Analysis” and the “Guidance note on the use of conflict analysis in support of EU External Action” were followed, focusing on the effects (the Branches of the Tree). To have a holistic view in the cyberspace in this war, it is important to know the cyber capabilities of the parts in conflict through trustworthy indexes like the Global Cybersecurity Index (GCI). This is issued by the International Telecommunication Union (ITU), the United Nations (UN) specialized agency for digital technology, and evaluates the countries' cybersecurity commitment toward a secure digital ecosystem, considering five pillars. The United States ranks first, Russia fifth, and Ukraine 78th, with capacity development being the weakest pillar. All the UN member states are committed to the United Nations' norms of responsible state behaviour in cyberspace with the Open-Ended Working Group (OEWG) on Information and Communications Technologies. Its approved report, published in March 2021, contains 11 voluntary and non-binding rules describing what states should and should not do in cyberspace.

Ukrainian cyberspace has been studied from different perspectives, including academic, military, and political perspectives. These include the cybersecurity system and the information warfare environment in Ukraine. Noteworthy are the 2015 and 2016 winters, when Ukrainian power grids were victims of disruption by proxy groups linked to Russia, which left a quarter of a million people in darkness and had a great impact on society due to the absence of energy for several hours. In 2017, the Notpetya malware, originating in Russia, caused losses of over $400 million and paralyzed a third of Ukraine's economy for three days. It also caused $10 billion in damage worldwide and was considered the "most destructive and expensive cyberattack in history. This malware affected companies worldwide, including WPP, Merck, and Maersk, amongst others, the latter with a loss of almost $300 million.

Looking at Russia's view on cyberspace, it can be divided into two levels: external, focusing on the Western public and decision-makers; and internal, focusing on Russia's efforts to ensure independence from the global Internet network. Russia sees cyber operations as an increasingly significant tool in the ongoing "information confrontation," which leads the NATO STRATCOM COE to consider that Russia explores cyberspace within a broad definition of the information domain, including both technical and psychological components. The digital transformation represents a world economy's objective for future sustainability development, and it is also part of the Moscow objectives for cyberspace. But numerous issues are preventing it from fully digitalizing, such as technical private companies including Google, Microsoft, PayPal, IBM, and CISCO leaving Russia due to the actual war.

Cyberspace security is also a European concern, with the EU Cybersecurity Agency (ENISA) providing annual reports on the status of cybersecurity threats. This war between Russia and Ukraine has reshaped the threat landscape, with geopolitics having a more substantial impact on cyber operations.

Interesting to note: the Ukrainian diaspora includes over 1 million Americans with Ukrainian ancestry and 20,000 Ukrainian immigrants living in California. Many of these immigrants work in Silicon Valley, which highlights the strong relations between the US and Ukraine and their technological affinity.

Since the Maidan events in 2014, Ukraine's tech sector has grown rapidly, creating a new class of young, wealthy workers with deep ties to the West. But also with this event, the hybrid threat environment increased in Ukraine, with manipulative and unwanted interference in society through various tools, including disinformation, historical narratives, election interference, cyberattacks, and economic leverage. The term "hybrid war" has become more familiar in the media environment, with articles in several occidental magazines highlighting the growing influence of Russia's hybrid activities against Ukraine. Following the recent invasion of Ukraine, Russia's cyberattacks have accelerated dramatically, namely with wiper malware to destroy data, threatening the Ukrainian internet and endangering vital information, services, and infrastructure.

The present reflection was conducted in the timeframe of October 2022 to February 2024. It considers the international support for Ukraine in cyberspace as the object of study and uses a qualitative research strategy based on a literature review. This analysis does not consider the dimensions of (dis)information and psychological warfare in cyberspace and is based on western and Ukrainian sources, therefore providing a non-global view of the facts needed for an independent analysis.

Institutional Support to Ukraine – Countries, Organizations and Companies

The international support for Ukraine has grown significantly since the invasion of Crimea in 2014, with cyberspace being part of it. Reports from the European Parliament show that Ukraine has suffered the most from cyberattacks since 2014, including phishing emails, denial-of-service attacks, data-wiper malware, backdoors, surveillance software, and information thieves. A Carnegie Endowment for International Peace report evaluates the international support for Ukraine in the context of cybersecurity, stating that a significant rise in capabilities and capacity has been achieved due to the worldwide effort to support Ukraine. A report of the Science and Technological Committee of the NATO Parliamentary Assembly provides an interesting view on four technological areas in this conflict, namely satellites, drones, mobile phone cameras, and cyberspace.

This document divides the support for Ukraine in cyberspace into two moments: before and after February 24, 2022, along with a note on hacktivism.

a. Before the invasion, some activities of the US should be highlighted: The FBI provided Ukrainian partners with direct support in law enforcement, assisting against disseminating disinformation, disrupting nation-state efforts, and exchanging investigative techniques on cyber incidents. Since 2017, the US Department of State has provided Ukraine with $40 million in cyber development assistance, and in 2020, it announced an additional $8 million in cybersecurity support. Between December 2021 and March 2022, US Cyber Command joint forces collaborated with the Ukrainian government to enhance cyber resilience in national critical networks. With around 40 US troops, the mission became one of its largest deployments, focusing on detecting harmful online activity on Ukrainian networks.
   Regarding International Organizations, the NATO support for Ukraine has two dimensions: capability development through the NATO-Ukraine Cyber Defence Trust Fund, which created laboratories as well as an incident management center; and technology support, with access to the NATO's Malware Information Sharing Platform (MISP), to facilitate information sharing on technical aspects of malware within the Allied community. On the European Union (EU) side, the most notable support is the €25 million project to aid Ukraine in its digital transformation and integration with the EU Digital Single Market. The Estonian E-Governance Academy has successfully carried out complex e-government projects in Ukraine since 2012. Coincidentally, a few days before the invasion, the EU Cyber Rapid Response Teams (CRRTs), a project developed within the EU's Permanent Structured Cooperation (PESCO) framework to respond to cyber incidents, were activated to help Ukraine's institutions in cybersecurity.

b. After the invasion, it is notable that there was great support from the western private sector for cybersecurity in Ukrainian companies and governmental institutions. Several companies, like Vectra AI, Avast, CrowdStrike, Cloudflare, CISCO, and Palantir, have offered services for network infrastructure scanning, endpoint protection, security solutions, as well as artificial intelligence software to support Ukraine's defense. But Amazon, Microsoft, and Google, as part of the five big technological companies known by the acronym GAFAM, should be more addressed due to their global market value and support for Ukraine.

   Amazon Web Services (AWS) has been instrumental in safeguarding crucial data in Ukraine's banking, educational, and government sectors. In February 2022, the same month of the Russian invasion, Ukrainian law was changed to allow the transfer of public and private sector data to the cloud, which belongs to private companies. After a Ukrainian government public plea for assistance to achieve that, AWS was one of the first firms to respond, securing, storing, and moving data to the cloud. Since the beginning of the war, Amazon has provided over $45 million in resources, goods, and cloud computing credits to local charities, and AWS has pledged $15 million in cloud computing credits and technical help. AWS has also supported Ukraine in migrating state registers and other vital state databases to the AWS cloud environment.
   Microsoft has introduced AI solutions to combat cybercriminals and protect clients' online activities. In response to the war in Ukraine, Microsoft reduced its business in Russia and pledged $100 million in technical assistance to Ukraine during the Lisbon Web Summit 2022, increasing its overall funding to over $400 million since the war began, in February. Through 2023 to 2024, Microsoft continued to provide Ukraine with free technology support. The company's Special Reports on Ukraine provide insights into Russia's use of cyber capabilities and offer strategic recommendations to organizations worldwide. In 2022, three reports were issued, providing strategic and technical details. The first report, "An overview of Russia's cyberattack activity in Ukraine," assessed the climate of urgency and warned of restricted capabilities like zero-days, attacks on infrastructure, and supply-chain attacks. The second report, "Defending Ukraine: Early Lessons from the Cyber War," highlighted the cyber components of the ongoing conflict and the unique characteristics of cyberspace. The last 2022

report, “Preparing for a Russian cyber offensive against Ukraine this winter”, issued in December, warns of a Russian cyber offensive against Ukraine, aiming to pressure domestic and international sources of support, initiating a hybrid campaign.
Google, the most popular website and search engine globally, has increased security measures to protect Ukrainian civilians and websites following the invasion. The company's President of Global Affairs, Kent Walker, announced measures such as SOS alerts, automated detection, Gmail notifications, increased authentication challenges, and the expansion of Advanced Protection and Project Shield programs. The Google Threat Analysis Group (TAG) is supporting in defence against sophisticated threats and state-sponsored malware attacks. Since Google acquired Mandiant, the company leader in Threat Intel and investigation in incident response services, it is providing better cybersecurity services to its customers and, consequently, to Ukraine.
In February 2024, Time magazine dedicated an edition to “How Tech Giants Turned Ukraine Into an AI War Lab”, where Steve Blank, a tech veteran and co-founder of the Gordian Knot Center for National Security Innovation at Stanford University, states that “This is the first time ever, in a war, that most of the critical technologies are not coming from federally funded research labs but commercial technologies off the shelf,” “And there’s a marketplace for this stuff. So, the genie’s out of the bottle.”

With a different approach, a special word must be given to **Starlink**, SpaceX's satellite network. This big private company, not IT but using cyberspace in its processes, aims to provide internet access to all of the Earth, especially to isolated areas. This enterprise has been enabling many Ukrainians, including the military, to stay online, despite power outages and Russian attacks on Ukraine's internet infrastructure. It is a secure satellite system that is easy to use, with an installation time of only 20 minutes. Over 25,000 Starlink terminals have been delivered to Ukraine by foreign partners, volunteers, or directly from SpaceX. The Starlink network has helped Ukraine win the drone war at the beginning of this conflict, as the Ukrainian military uses "Delta" technology to locate and destroy invading forces. Ukrainian soldiers could use drones to relay data to Command and Control (C2) centers and organize strikes against Russian military troops. The Delta, a situational awareness and battlefield management system developed and used in Ukraine, has been tested at the Sea Breeze military exercises, in the Black Sea. This is a series of multinational maritime exercises, led by the USA, to improve interoperability with NATO systems. Without Starlink's early and cheap access, Ukrainian networks could not have survived.

Some International Organizations have also providing/continued to provide support to Ukraine. **NATO** support for cyberspace includes Ukraine's admission to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in 2022. The CCDCOE provides interdisciplinary expertise in technology, strategy, operations, and law. Regarding support with cyber threat intelligence or other kinds of information, it can be considered part of the NATO position in this conflict. By its side, the **EU** has invested over €10 million in Ukraine to enhance cybersecurity and maintain public services, with the "EU Support to Strengthen Cyber Security in Ukraine" project in 2022. Next year, more 17,4€ million will be allocated to the project “Digital Transformation for Ukraine (DT4UA). The European Union Agency for Cybersecurity (ENISA) has formalised a Working Arrangement with its Ukrainian counterparts focused on capacity-building, best practices, and situational awareness.

Considering the support provided by countries, two can be underlined: the **US**, which has added $45 million to Ukraine's cybersecurity defense in 2022, enhancing its cyber-defensive capabilities. The Cybersecurity and Infrastructure Security Agency (CISA) signed a Memorandum of Cooperation with the Ukrainian State Service of Special Communications and Information Protection of Ukraine to provide warnings preventing malware targeting Ukrainian enterprises. In the intelligence services,

the US has also been actively disclosing Indicators Of Compromise (IOCs) from Ukrainian networks, serving as digital forensics for network defenders and proof of Russian intrusions. And the **UK**, with the Ukraine Cyber Program, funded by £6.35 million, which aims to protect Ukraine's government and infrastructure from cyberattacks following Russia's invasion. This program, involving industry collaboration, also aims to prevent malicious actors from accessing key networks.

c. On the Ukrainian side of strategic decisions, the volunteer IT Army to fight Russia online is an example, targeting railways, the energy grid, and governmental and financial institutions. This army, which has thousands of cybersecurity professionals, is part of the "digital war" against Russia. The number of IT soldiers is unknown, but by the end of February 2022, 175,000 people had subscribed to the public channel provided by the Ukrainian government. The IT Army volunteers have different motives, expertise, and abilities to use cyber weapons. Anonymous is a powerful player in Ukraine's cyber guerrilla army, hacking over 300 Russian cyber targets in 48 hours. However, Tim Stevens, a senior lecturer in global security at King's College London, warns of unexplored and hypothetical scenarios when it comes to cyberattacks and the possibility of escalation. Another apprehension is with cybercrime, with the world of cybercriminals currently divided between supporters of Russia and Ukraine. Rob Joyce (NSA-USA) and Lindy Cameron (NSCS-UK) have alleged that Western nations are concerned about the resurgence of hacktivists.

To close this theme, and taking into consideration reports from the International Institute for Strategic Studies (IISS), Chatham House (CH), European Parliament (EP), Carnegie Endowment for International Peace (CEIP), the European Cyber Conflict Research Initiative (ECCRI), and the Center for Strategic and International Studies (CSIS), some key takeaways and extracts can be presented:

- The fundamental goals of wartime operations—sabotage, influence, and espionage—have remained unchanged (ECCRI).
- Ukraine has successfully resisted Russian cyberattacks thanks in large part to assistance from its international allies as well as—and this is crucial—the private sector (CH).
- Due to their significant engagements in the conflict, digital corporations have been highlighted as geopolitical actors as a result of the war: these companies' direct offering of cyber-security services and capabilities has supported Ukraine's cyber defense during critical times; and due to their withdrawal from Russia after the invasion, tech corporations have damaged Russia's economy and prestige (IISS).
- Russia launched a persistent effort to breach and interfere with Ukraine's vital national infrastructure, but defense dominated the majority of the effort since it had access to excellent intelligence and world-class cyber-security knowledge (IISS).
- The incapacity of Russia to coordinate cyber operations with other military impacts, the poor state of its own cyber security, and the absence of the skills necessary to surgically disable military combat targets are the main shortcomings in Russian cyber capabilities when compared to those of the US (IISS).
- It is getting more and more difficult to differentiate political activist groups from cybercriminals, which undermines the notional protection they are afforded as civilians rather than combatants (CH).
- The (Cyber) Confrontation will not end with a ceasefire (CEIP).
- In large theater wars, cyber activities will be supportive rather than decisive (CSIS).
- War will continue to be a tool for advancing politics, depending more on the visible results of bloodshed than on the less obvious consequences of breaking into communication networks (CSIS).
- Because they enable a non-violent engagement that uses covert action, propaganda, and monitoring in a way that fundamentally threatens human rights, cyber operations continue to be valuable as a tool of political warfare. Cyber operations will remain a limited tool of coercion (CSIS).

3. Gaza

Moving now to the actual conflict in Gaza, where Israel is at war with Hamas, in cyberspace, it is worthwhile to mention two reports issued in February 2024. One by Google Threat Analysis Group and Mandiant, based in operations by six regional threat groups with ties to Hamas, Hezbollah, and Iran. The main activities conducted were cyber espionage, information operations, and potentially destructive activities. In this case, the cyber operations did not play a supporting role like they did in the beginning of the Russian offensive in Ukraine, being used independently. Iran, a long-standing adversary of Israel and the US, continues its cyber operations. In the six months leading up to the Hamas attack, Iran was responsible for about 80% of government-sponsored phishing activity targeting Israeli users.
The other report, by the Microsoft Threat Analysis Center (MTAC), highlighted that Iran has conducted cyber-enabled influence operations in support of Hamas during the Israel-Hamas war. These operations combine offensive cyber activities with messaging to shift perceptions and behaviors. Three phases could be considered: (1) Reactive and Misleading: Initially, Iranian groups were reactive, exaggerating the scope and impact of claimed cyberattacks, however there's no clear evidence of coordination with Hamas before the October 7 attack; (2) Targeted Influence Tactics: Iran's influence operations have sought to intimidate Israelis, criticize the Israeli government, and undermine support for Israel's military operations and (3) Growing Threat: As the conflict persists, Iran's cyber and influence operations are expected to escalate, especially amid the potential for a widening war. Note: a Gaza-based threat actor known as Storm-1133 has targeted Israeli private-sector energy, defense, and telecommunications organizations.
Also noteworthy: the news report of a US cyberattack launched on an Iranian military ship that was gathering intelligence on cargo ships in the Red Sea and Gulf of Aden. The operation was designed to prevent the Iranian ship from sharing intelligence with Houthi rebels in Yemen, who have been shooting missiles and drones at cargo ships in the Red Sea. According to several international independent journalists, namely The Guardian, New York Times, The Walrus, Le Monde, CNN, or France 24, amongst many others, Israel is using Artificial Intelligence as a "Weapon of War". And according to The Jerusalem Post, an IDF Intelligence Corps senior officer said, "For the first time, artificial intelligence was a key component and power multiplier in fighting the enemy". This is of great concern, when a machine has the power to decide on targets, where there are civilians.
Meanwhile, it is possible to see a direct dispute between Israel and Iran in cyberspace, below the threshold level of war, trying to disrupt societal systems in both countries, with hacktivism on the rise supporting both sides of the conflict.

4. To conclude Ukraine and Gaza

Cyberspace is part of two conflicts with different approaches, due to the different capabilities of its actors. In Ukraine, the belligerent parts are not following the commitment to the United Nations' norms of responsible state behaviour in cyberspace. The United States is a global actor, participating in the two conflicts. Hacktivism has been growing, aiding both sides in the two conflicts. Artificial Intelligence is also part of them, with different approaches, one being part of the market looking for profits with "the genie's out of the bottle" and the other using it for killing purposes.

Eurodefense, Portugal

Geostrategic position of Portugal in the global submarine cable network. Challenges and Opportunities

COL Luís Bernardino[1]

lbernardino@autonoma.pt

"*...We currently live in a changing world where the control of large maritime spaces has become a priority for States, especially when there is a concern for sovereignty over these spaces and we intend to monitor everything that can contribute to our sustainable development. In Portugal. The "new" SMART Cables technology will be a relevant contribution to this goal. In this opinion article we intend to raise some key questions and contribute to a debate that we believe to be useful and very necessary for the development and security in Portugal and in the world...*".

BARROS, José & BERNARDINO, Luís M. Brás (2023). "Contributions of SMART CABLES technology to sustainable development in Portugal". In Jornal da Economia do Mar.

Introduction

Submarine cables are crucial to cyberspace's cybersecurity, acting as the backbone of global internet connectivity and data access. These subsea cables carry vast amounts of data between continents, facilitating seamless communication and access to online services essential to our society. Protecting the security of these cables is imperative due to their vulnerability to physical and cyber threats, such as sabotage, espionage, and disruptions. Therefore, safeguarding submarine cables is vital for maintaining critical infrastructure, economic stability, and national security.

Modern submarine cables utilize fiber-optic technology capable of transmitting multiple terabits of data per second. Lasers on one end send data at extremely rapid rates through thin glass fibers to receptors at the cable's other end. These glass fibers are protected by layers of plastic and sometimes steel wire. Submarine cables consist of copper or optical fibers, encased in several protective layers of plastic, wire, or synthetic materials. These cables can stretch up to 11,000

[1] Luís Manuel Brás Bernardino is a Portuguese Army Colonel (Reserve) with more than 37 years of experience in UN, NATO and EU missions. Graduated with the Staff Course and the National Defence Course, holds a master's degree in Strategy and a PhD in International Relations from the Lisbon University. Professor at the Military University Institute with extensive international experience on teaching, training, and advising. Regularly participates in conferences, evaluation boards, and other academic or institutional events related with submarine cables and global interconnectivity. Professor at the Department of International Relations at the Autonomous University of Lisbon. lbernardino@autonoma.pt

km in length and reach depths of 8,000 meters. Installing and operating these systems can take several years, with a lifespan of approximately 25 years.

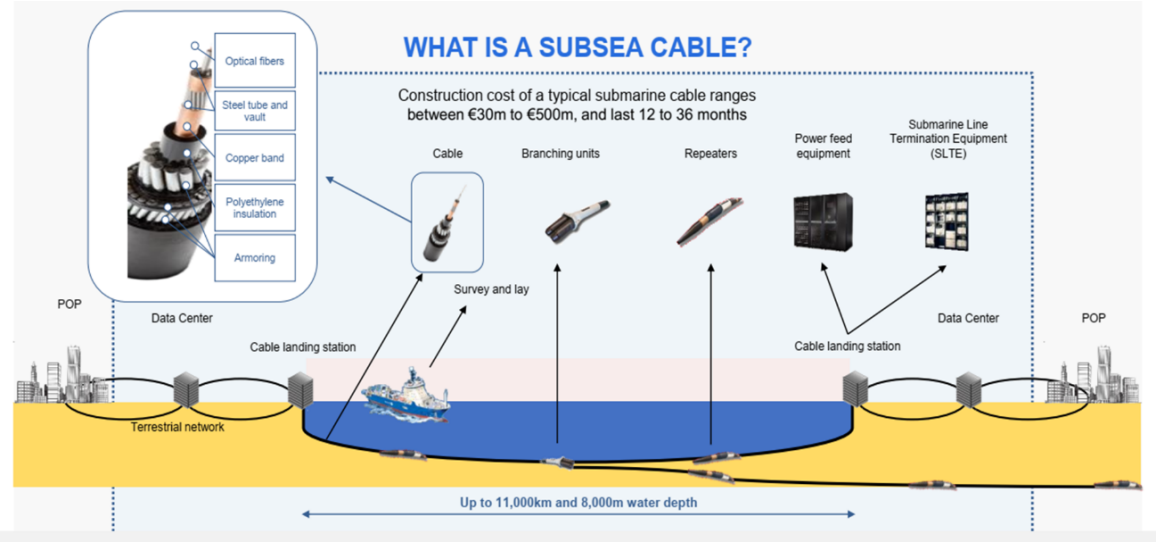

Figure 1 - Subsea Cable

(https://www.csis.org/analysis/securing-asias-subsea-network-us-interests-and-strategic-options)

The 2AFRICA[2] submarine cable, the world's largest, spans 45,000 km, encircling Africa and connecting 46 landing points across 33 countries, including the United Kingdom, India, and numerous countries in the Middle East and Africa. At 45,000 km in length, 2AFRICA is one of the world's most extensive subsea cable projects, interlinking Europe (eastward through Egypt), Asia (via Saudi Arabia), and Africa.

The system was scheduled to go live in 2023, offering a design capacity of up to 180 Tbps—surpassing the total combined capacity of all existing subsea cables serving Africa. 2AFRICA will provide essential internet capacity and reliability across extensive regions of Africa, meet the rapidly growing capacity demands in the Middle East, and support the expansion of 4G, 5G, and fixed broadband access for billions of people.

Past to the Present...and what about the future?

Specialists categorize the history of deep-sea communication into three periods: the Telegraph Era (1845-1929), the Telephone Era (1930-1985), and the Digital Age (1988-present). The first submarine Atlantic telegraph connected England to America, crossing the Atlantic and linking Lisbon (with Carcavelos as the first landing station in Portugal) and the Azores to the world. In the early days, Portugal emerged as a central hub for sea cable communication. After 1910, telegraph lines proliferated across the northern Atlantic Ocean, establishing that region as the focal point for cable communication, connecting America to Europe and Europe to the rest of the world.

More recently, in the digital age after 1990, we have witnessed the globalization of submarine cables. Global enterprises and communication companies have become more influential than states, with the liberal market driving the worldwide development of submarine cables. The internet, which we rely on for daily activities, depends on these subsea cables to deliver data to

[2] https://www.2africacable.net/

users promptly, whenever and wherever needed. Over the past decade, global interconnectivity has more than doubled, with key areas of sea cable development including the North Atlantic, connecting the US with Europe, the Pacific region in Asia, and the Middle East.

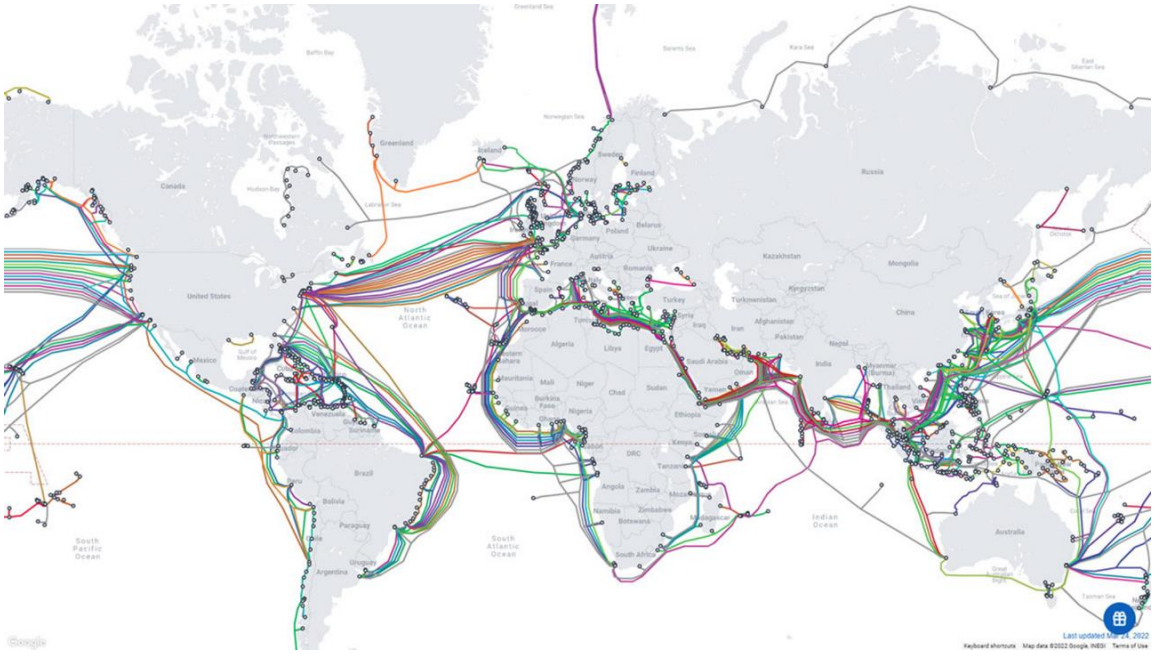

Figure 2 - Subsea Cables Map (www.telegeography.com)

Global internet traffic is forecasted to continue growing over the next few years, with an expected increase of at least 20-25%. However, there is a significant possibility of a data volume explosion if certain innovative technologies gain sudden popularity. For instance, artificial intelligence will demand a higher level of data, speed, and complexity within the digital ecosystem. Individual internet usage is also set to rise, further increasing our dependence on the internet.

We rely on the internet for accessing and providing information, entertainment, gaming, and, most importantly, communication. Europe currently leads in individual internet usage, while Africa is poised to experience the fastest growth rate. Asia and America are also in the race, with Europe continuing to serve as a strategic hub for communications, as it has in the past. This hub provides internet services to Asia, the Middle East, Africa, and Europe. Portugal, situated at the center of this hub, faces both significant opportunities and challenges.

With the continuous global increase in internet demand, the need for submarine cables is also rising significantly. In 2022, there were 530 active submarine cables worldwide. This number grew to 552 in 2023, and by early 2024, we have already reached 574 active cables globally.

As of early 2024, it is estimated that there are 1.4 million kilometers of submarine cables in service worldwide. Some cables are relatively short, such as the 131-kilometer CELTIX Connect cable between Ireland and the United Kingdom. In contrast, others are extremely long, like the 20,000-kilometer Asia America Gateway cable. While submarine cables are economically significant, data centers (represented by green dots in the picture below) are equally important. Portugal should aim to become a hub for data centers, capitalizing on the information economy rather than merely serving as a transit point for submarine cables.

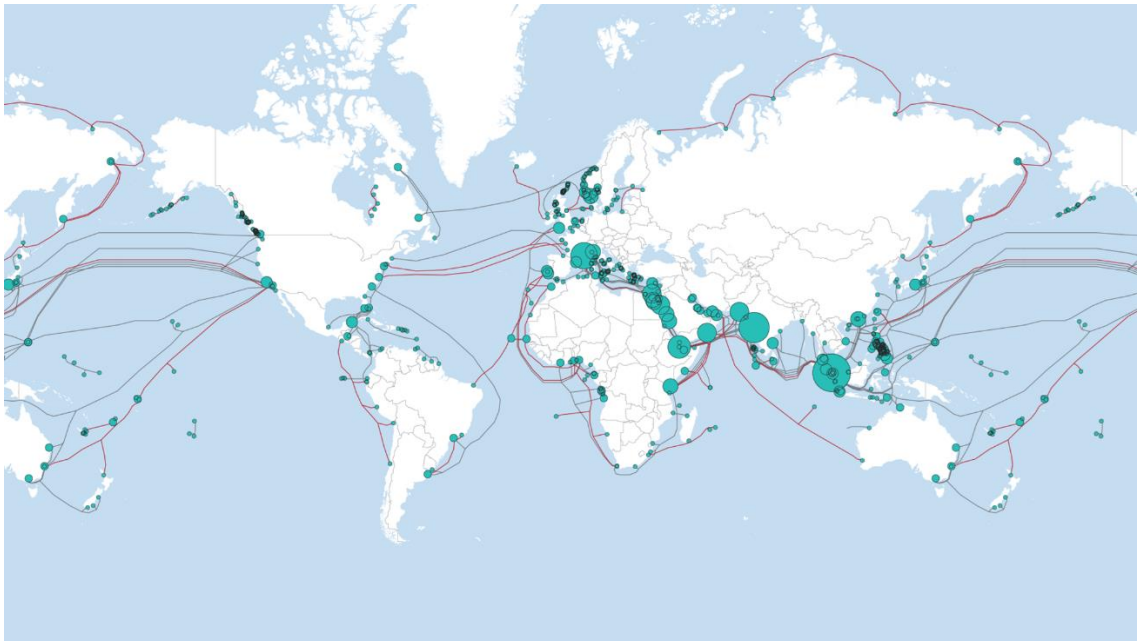

Figure 3 - Subsea Cables and Datacenters Mapping (www.telegeography.com)

Geostrategic position of Portugal in the global submarine cable network

Portugal's geostrategic position in the global information network is significant, with about 25% of sea cables crossing its Exclusive Economic Zone (EEZ) and around 75% of submarine cables crossing the North Atlantic passing through its waters. Until 2023, Portugal was the only country in the world with direct sea cable connections to all continents. In the next 2-3 years, several important submarine cables will be installed in Portugal, including "NUVEM" (2026), "2AFRICA" (2024), and the "ATLANTIC CAM," which will establish new connections between the mainland and Madeira and the Azores using SMART Cables[3].

Portugal's sea cable landing stations are currently concentrated in just four locations near Lisbon and around 100 kilometers south, which poses a significant vulnerability. Specialists suggest diversifying and establishing additional landing stations along the northern coast, equipped with power supply infrastructure and mega data centers. For example, Sines already has multiple HDD bore pipes at the beach to support future systems landing there. From a terrestrial perspective, Sines offers a robust network solution with diverse backhaul routes to Lisbon and Madrid, running over gas pipes and power lines. The opportunities and challenges in this area depend on the level of political engagement and strategic involvement of national and especially international partners.

[3] https://www.jornaldaeconomiadomar.com/contributions-of-smart-cables-technology-to-sustainable-development-in-portugal/

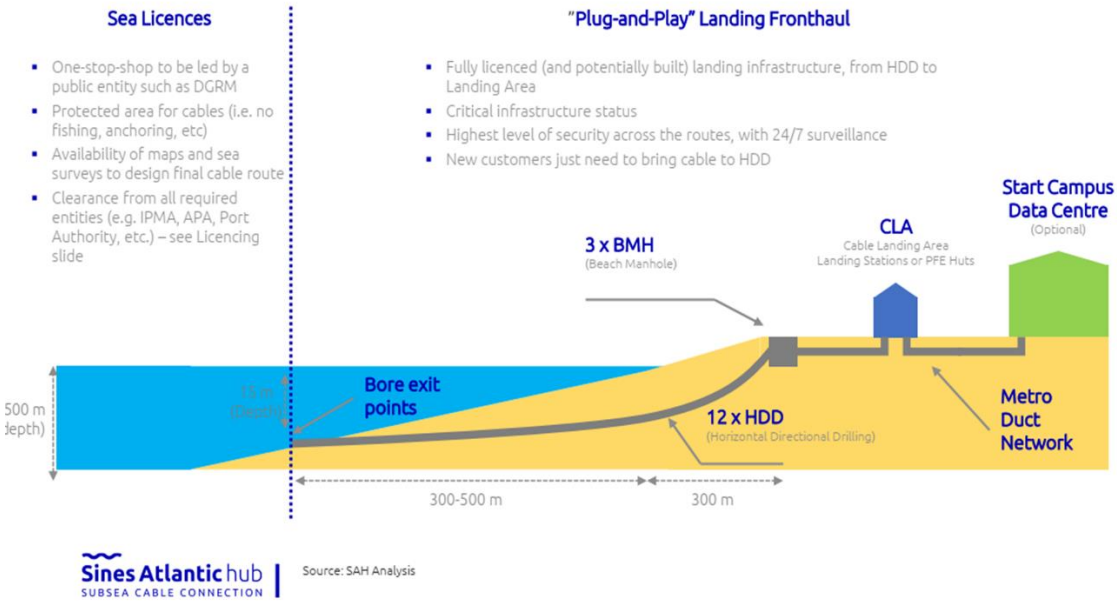

Figure 4 - Sines Subsea Cable Connection (https://www.startcampus.pt/en)

Conclusion

Portugal's geostrategic position is unique, offering North-South Atlantic interconnections with access to Africa and South America, East-West connections to North America, and links to Europe and the Mediterranean Basin, extending to the Middle East and Asia. Remarkably, Portugal is the only country in the world with direct underwater cables moored to all continents, except for Antarctica.

Portugal enjoys numerous advantages due to its geographic position, but more needs to be done in terms of national strategy to transform these advantages into economic opportunities. To achieve this, Portugal must focus on strategic cooperation between states and companies and lead the global dialogue on subsea cables. By doing so, it can become a strategic partner and one of the most influential countries in the world in the near future.

Bibliography:

https://www2.telegeography.com/hubfs/LP-Assets/Ebooks/state-of-the-network-2024.pdf?

https://www.submarinecablemap.com/submarine-cable/2africa

https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2022)702557

https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf

BARROS, José and BERNARDINO, Luis Brás (2023). Contributions of SMART CABLES technology to Sustainable Development in Portugal. In Jornal da Economia do Mar. 2023. https://www.jornaldaeconomiadomar.com/contributions-of-smart-cables-technology-to-sustainable-development-in-portugal/

KRAUS, C., and CARTER, L., (2017). A Bibliography of Submarine Communication and Power Cables. International Committee for Protection of Cables (ICPC) Publication June 2017, 25pp. https://www.iscpc.org/publications/

BUEGER, C. and Edmunds, T. (2023) "The European Union's Quest to Become a Global Maritime-Security Provider," Naval War College Review: Vol. 76: No. 2, Article 6. Available at: https://digital-commons.usnwc.edu/nwc-review/vol76/iss2/6

Josef Schroefl
ORCID No: 0000-0002-6988-1737

HYBRID THREAT SCENARIO AND ITS DEVELOPMENT DURING HYBRID CAMPAIGNS WITH SPECIAL CONSIDERATION OF CYBER POWER

Abstract

Growing dependence on information technology and the interconnection of critical infrastructure have made a secure cyberspace vital to the functioning of a modern state. This article will showcase how dependency on cyberspace is continuously increasing and it will outline recent developments as they pertain to hybrid threats emanating from cyberspace. This paper will demonstrate how the dependency on cyberspace and the ability of aggressive actors to use cyber-power to magnify the cumulative effects of certain activities to create a hybrid effect that becomes a security threat. The ubiquitous nature and access to cyberspace is the force multiplier for activities that might on their own, and viewed discretely, seem less consequential. The combination of Cyber Power and Hybrid-threats represents an explosive blend of factors that has enabled adversaries to leverage their relatively meager resources. For Western strategists and decision makers, this means that the apparently and traditionally weaker part of the adversarial equation has now received additional advantages and opportunities through the hybridization of conflict. Using scenarios and examples, the article describes the what extent hybrid threats can affect peace and prosperity of our societies. The scenaric description of hybrid influencing can be roughly divided into three phases: Preparation – Destabilization – Violence and military activities[1].

Keywords: Hybrid, Cyber, threats, campaign, scenario

Introduction

Roughly summarized, hybrid threats can be summarized as strategies in which attackers are banking initially on a combination of propaganda in the media and social networks until ultimately relying on classic warfare.

The use of these hybrid strategies has dominated the security policy debate worldwide in the last years. In the beginning, hybrid threats were often seen as a new topic, but they are not.

[1] A shorter extract from this article has already been published in English and Finnish language in Cyberwatch Finland 2024, No2, p. 12 - 17

They are as old as conflicts and wars themselves, but repackaged and supported by innovative tools, concepts, strategies and technologies that uniquely target the weaknesses of our western societies. They are directed against the functioning of the state and its institutions and thus also against the sovereignty of a country.

Although the "classic warfare" remains up-to-date, the new hybrid means of exercising power increase the reach and effectiveness in achieving strategic goals. In the case of hybrid threats, internal and external security are closely linked and often occur where they overlap[2].

Hybrid and cyber threats

While definitions of hybrid threats vary and must be flexible in order to describe their evolving nature, hybrid treats cover the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare[3]. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder an adversary's decision-making. Energy Infrastructures are targets of vital importance[4] .

Hybrid-threats but also refer to the methods and tools used by individual state or non-state actors to enhance their own interests, strategies and goals. The range of methods and activities is wide: influencing information and propaganda, logistical weaknesses like energy supply pipelines, economic and trade related blackmail, undermining international institutions by rendering rules ineffective, terrorism, increasing insecurity (border incidents like airspace violations without admission, talking about legitimate interests, immigration questions) etc.

There are state and non-state actors that are challenging countries and institutions they see as a threat, opponent or competitor to their interests and goals. The range of methods and activities is wide, including: influencing information; logistical weaknesses like energy supply pipelines; economic and trade-related blackmail; undermining international institutions by rendering rules ineffective; terrorism or increasing insecurity.

Hybrid threats are methods and activities that are targeted towards vulnerabilities of the opponent. Vulnerabilities can be created by many things, including historical memory,

[2] See also Josef Schröfl, *Cyber power is changing the concept of war*, "Hybrid CoE strategic Analysis", 21, Helsinki/FIN, March 2020, pp. 2-3.

[3] See also Sascha-Dominik Bachmann, *Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats – mapping the new frontier of global risk and security management*, January 2012; https://www.researchgate.net/publication/228214544 (last accessed on 21. May 2020).

[4] According to the EU: *Joint Framework on countering hybrid threats*; https://eur-lex.europa.eu/legal-content/EN (last accessed on 21. May 2025).

legislation, old practices, geostrategic factors, strong polarization of society, technological disadvantages or ideological differences. If the interests and goals of the user of hybrid methods and activity are not achieved, the situation can escalate into hybrid warfare where the role of military and violence will increase significantly.

Accordingly, the Hybrid CoE characterizes hybrid threats as[5]:

- Coordinated and synchronized action, that deliberately targets democratic states' and institutions systemic vulnerabilities, through a wide range of means,
- The activities exploit the thresholds of detection and attribution as well as the different interfaces (war-peace, internal-external, local-state, national-international, friend-enemy),
- The aim of the activity is to influence different forms of decision making at the local (regional), state, or institutional level to favour and/or gain the agent's strategic goals while undermining and/or hurting the target.

Cyber-threats in a hybrid threat strategy are the *power of the weak*, and when effectively used can give significant advantages to the *weaker side* as well as create a future conflict potential where military instruments will also be deployed.

The cyber domain and activity in cyberspace do not automatically constitute a hybrid threat. In the landscape of hybrid threats, cyber is only one domain of many in which harmful activity can take place. Cyber interference consists of operations by state or non-state actors conducted in cyberspace. If this activity targets critical infrastructure, for instance, by cyber means to achieve political/military aims alongside other activity by an outside hostile actor – we have hybrid action. Cyber interference, in its priming phase, can effectively spy on and manipulate electronic and information systems. At this juncture, it would be premature to talk in terms of waging war. It is not possible at this point to know whether the activity will escalate into war. However, as hybrid activity blurs the real aims and goals of the activity, it might force us to make hasty and poor decisions.

For several years, the term "Hybrid-threats" has been used more and more to explain the nature of threats, including the nature of war. However, this inflationary use and monograph also calls into question the meaningfulness of use to characterize the threats we face.

It seems all the more important to clarify the ambiguities at the strategic level in order to make the unclear visible, which, however, threatens to blur in the event of threats from cyberspace or Hybrid-threats. Such vagueness is most clearly expressed when the scientific

[5] https://www.hybridcoe.fi/hybrid-threats/ (last accessed on 21. May 2025).

debate speaks of Hybrid-threats and refers to cyberattacks what are only part of a wide spectrum of hybrid means.

Hybrid threat scenario

Although the USA, closely followed by China and Russia, are still possessing the superiority in the field of conventional weapon systems, - and arms spending worldwide increases year after year, crises and conflicts carried out conventionally are no longer the most likely form of conflict resolution. States and societies are still, but less and less threatened by "classic" weapon systems than by the possible multiple use of hybrid means.

The scenaric description of hybrid influencing can be roughly divided into three phases:

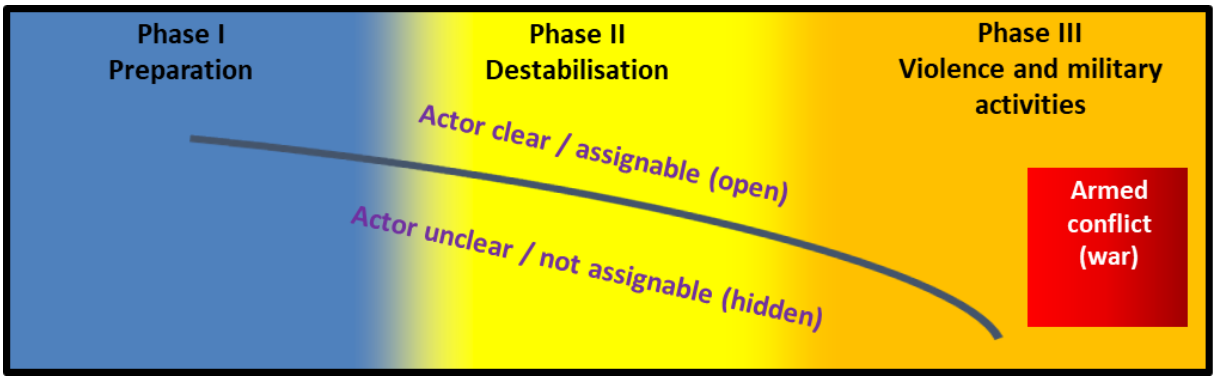

Figure 1: This graphic is intended to illustrate that at the beginning of hybrid influencing, the aggressor is unknown. But as longer the attacks continue, target and nature of the attacker becomes clear

Phase 1 - preparation:

This phase is starting already in times of deepest peace, can extend over years and is characterized by blurring traditional dichotomies and creating ambiguities. Individuals and societies have an inherent preference for thinking in dichotomies (truth / lie, friend / enemy, etc.) and our decision making is largely based on this way of thinking. On the other hand, ambiguities hinder decision-making at the individual and collective levels by creating confusion and distrust. Through well-coordinated disinformation campaigns, the aggressor causes ambiguities that impair judgment and trust in political or social actors and institutions and begin to undermine. Basic knowledge and thus checking the truthfulness of statements takes a back seat. Being "under the radar" as much as possible so as not to be recognized and to obscure the targets is one of the characteristics of hybrid activities in this phase.

Action:

Politicians, political parties or communities of interest are being discredited, their reputation will be undermined by using “fake new”. False information is consistently published by manipulative intent in the public media and on the Internet, especially in social media, which are particularly suitable for this, since they have developed into a preferred source of information in the digital world[6]. This is exemplarily done by:

• Publication of falsified or correct personal data such as health data, statements / deeds / events from the past in order to discredit people.

• Data leaks, for example to disclose financial transactions by individuals and / or groups / parties, to manipulate them or to represent them as manipulated. This can be done by buying a "mole" from inside or anonymous hacker attacks from outside. "False flag" attacks, i.e. attacks under the false flag can also be assumed.

• Critical articles and statements on the Internet about the aggressor will be remarked with hate and false comments, provided from "Troll factories".

Phase 2 - Destabilization

Continuing with phase 1, that phase is characterized by further undermining public confidence in democratic institutions, manipulating democratic decision-making, questioning basic values of the society, and goes up to attacks against strategic infrastructures as well as impairing the decision-making ability of political leadership. The basic values of Western societies and democratic decision-making such as freedom, the rule of law, equality, individualism, openness and tolerance are manipulated in order to endanger these values. While in phase 1 the aggressor tries everything to disguise himself and his goals, in phase 2 the fog of anonymity around the attacker and his goals is increasingly cleared.

Action:

In principle, the attacker will try to create further political, economic and / or military conditions for the internal destabilization of the attacked states / society in this phase. It is usually initiated by an extraordinary event, whether natural or man-made. This can be a natural disaster (e.g. large-scale flooding or earthquake), the outbreak of an epidemic / pandemic like we saw it in 2020 with the COVID-19 pandemic and / or a terrorist attack. Ideally, the state under attack is also in a period of upheaval, such as the uncovering of a serious scandal, new elections or the

[6] *The revelations and indictments about the Russian involvement with the 2016 United States presidential election highlights how digital attacks can be used against intangible targets, such as faith in social and traditional media, and confidence in the integrity of elections*, citated from Fahmida Y. Rashid in: *From Disinformation as a Form of Cyber Attack*, published in Decipher; https://duo.com/decipher/disinformation-form-cyberattack, accessed: 15.09.2025.

phase of forming a government. The aim is to increase unrest and massive protests among the population in order to gradually cause chaos. Nonviolent protest, especially at the end of this phase, turns into violent resistance:

• Further intimidation, extortion, deception and / or bribery of political opponents, parties, organizations, media, journalists, etc. by the aggressor,

• Infiltration, and subsequently funding of parties / institutions / NOGs / individuals that serve the interests of the aggressor,

• Support for ethnic, religious and / or social groups, which generally appear disaffected and disillusioned. Infiltration and instrumentalization of their interest groups to further fuel dissatisfaction. Increasing using them as a "proxy" (Proxies are entities that have a favorable opinion for a foreign state or whose own interests bring them into harmony with that state – the fifth column) for the interests of the aggressor. The range is from paramilitary organizations to political parties, movements and individuals,

• Introducing / promoting militant groups and reinforcing subversive actions,

• Acts of terrorism against individuals and / or critical infrastructures such as electricity and water utilities, but also against cultural assets and national / social symbols,

• Cyber-attacks to disrupt the communication infrastructure, such as TV, radio and / or telecommunications (cell phone networks, etc.),

• Cyber-attacks against critical infrastructures such as airports, power plants and other facilities, will create significant supply bottlenecks or threats to public security,

• Hamster purchases by the population lead to further supply shortages,

• The government starts to deploy the armed forces to assist and support its own law enforcement (police).

Phase 3 - Violent clashes up to war

The logic of a presumptive opponent in this phase is escalation of violence. While all tactics of the hybridization of phase 1-2 continue, the state crisis can develop in this phase from regionally limited civil clashes to an open armed conflict/war. The worst-case scenario would occur if armed groups are using weapons of mass destruction to pursue their targets and / or a comprehensive destruction of the critical infrastructure with a final blackout succeeds.

Action:

• At the beginning of this phase, logistic support (money, weapons, equipment, personal, etc.) will be provided by the aggressor to groups, ready for violence,

• Possible necessary military actions of the attacker in their own territory will be prepared. Private combat groups and special commandos will be transferred (open or hidden) into the country to support the armed opposition,

• Violent clashes are taking place between the state law enforcement and demonstrators or groups. The first lootings will occur,

• The law enforcement cannot longer control the increasing willingness to use violence; the army, which already assists, will be fully mobilized.

Conclusions

Hybrid threats initially target intangible assets and develop into attacks on the sovereignty of states - with far-reaching economic, political and social impacts. • Many options for hybrid influencing on states / societies, such as long-term and large-scale industrial and financial manipulations, are currently barely perceived in the context of hybrid threats - but could drastically change the geostrategic balance of power. If a country is sufficiently resilient, however, the hybrid attacks can be recognized early and thus stopped. If a crisis, as exemplified, escalates and national resources are insufficient, citizens expect NATO or the EU to provide aid, which must therefore already reorganize the relationship between resilience, deterrence as well as security- and defense policy. As a *worst case* remains a comprehensive blackout in connection with armed conflicts on one's own territory. That this will not happen, the coordinated use of all government instruments, including the armed forces is required. The use of hybrid strategies thus makes it clear, that the whole-of-government approach must be adapted, organized and developed into a whole-of-state / society approach.

References

Axelrod, Robert, *The Dissemination of Culture: A Model of Local Convergence and Global Polarization*," Journal of Conflict Resolution", 1997, 41(2), pp 27 - 75

Bachmann, Sascha-Dominik, *The current crisis in the Persian Gulf in the context of hybrid warfare*, Researchgate, Berlin, 2018.

Gray, Colin S., *Making Sense of Cyber Power: Why the Sky Is Not Falling*, Carlisle, PA: Strategic Studies Institute, 2013.

Hoffmann, Bruce, *Inside Terrorism*, "Columbia Studies in Terrorism and Irregular Warfare" 2006, pp. 7 - 104

Libicki, Martin. C., *Cyberdeterrence and Cyberwar*, RAND Corp., London, 2009.

Münkler, Herfried, *Die neuen Kriege*“ Reinbek, Berlin, 2002.

Pfetsch, Frank R. and Christoph Rohloff, Kosimo, *Databank of Political Conflict*, “Journal of Peace Research” 2000, 37(3), pp. 34 - 67.

Schröfl, Josef, Stuart J. Kaufman, *Hybrid Actors, Tactical Variety: Rethinking Asymmetric and Hybrid War*, “ Studies in Conflict & Terrorism” 2014, no 37, pp 862–880

Schröfl, Josef, *Cyber power is changing the concept of war hybrid*, CoE Strategic Analysis 21, Helsinki/FIN, March 2020.

Wendt, Alexander, *Anarchy is What States Make of It*, “International Organization” 1994, no 46(2), pp. 44 - 82