Naif Arab University for Security Sciences
Journal of Information Security & Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

From Prevention to Resilience: Operational Tactics and EU Cybersecurity Frameworks

Jersain Zadamig Llamas Covarrubias
Division of Legal Studies, University Center of Social Sciences and Humanities, University of Guadalajara, Guadalajara, Jalisco, Mexico.

Received Jan. 2025; Accepted 25 May. 2025; Available Online 29 Jun. 2025

Abstract

Cyber threats continue to outpace conventional defense strategies, underscoring the need for more adaptive security approaches. This study examines how six principal European Union frameworks, including the Network and Information Security Directive (NIS2) and the Digital Operational Resilience Act (DORA), align with modern operational tactics: Redirect, Obviate, Impede, Detect, Limit, and Expose. Using a structured qualitative methodology, including legislative text analysis and cross-referencing with real-world incidents, the research maps each regulation's provisions to specific defensive functions. Results indicate that while prevention, detection, and coordinated incident response are well addressed, more assertive tactics, such as diverting attackers to decoy environments or employing strategic deception, remain largely absent. This gap may limit the EU's overall capacity to counter sophisticated threats that circumvent static defenses. In conclusion, supplementing existing regulations with practical guidance and controlled pilot initiatives could enhance cyber resilience without compromising legal or ethical standards. Such measures would empower both public and private entities to adopt a broader range of defensive strategies, ultimately strengthening Europe's posture against increasingly advanced cyberattacks.

I. INTRODUCTION

In today's cyber threat landscape, malicious activities have escalated well beyond basic unauthorized access attempts. Adversaries are increasingly sophisticated, leveraging stealthy tactics, advanced persistent threats (APTs), and complex intrusion methods that demand more than traditional, preventive-focused security measures. While firewalls, antivirus software, and network segmentation remain important first lines of defense, such passive controls alone are insufficient against adversaries adept at circumventing static barriers.

Resilience-based strategies are therefore emerging as essential complements to conventional prevention. By integrating operational tactics — Redirect, Obviate, Impede, Detect, Limit, and

Keywords cyber defense strategies, cybersecurity resilience, EU regulations, information security, operational tactics

Production and hosting by NAUSS

*Corresponding Author: Jersain Zadamig Llamas Covarrubias
jersain.llamas@academicos.udg.mx

doi: 10.26735/VVMS1897

Expose — organizations can better detect, disrupt, and recover from attacks. These high-level tactics encompass subcategories like Deter, Divert, and Deceive, which actively shape adversarial behavior by increasing the costs and risks associated with mounting an attack. Crucially, such an approach shifts cybersecurity from a reactive posture to a comprehensive, adaptive model that anticipates threats, sustains vital functions, and expedites recovery when breaches occur.

Concurrently, the European Union (EU) has instituted a robust legal and regulatory framework, most prominently through the NIS2 Directive, the Digital Operational Resilience Act (DORA), the Cyber Resilience Act (CRA), the Cybersecurity Act (CSA), the Critical Infrastructure Directive (CID), and the Cyber Solidarity Act. Collectively, these instruments aim to strengthen organizational readiness, foster cross-border cooperation, and elevate cybersecurity standards within and across Member States. However, despite clear progress in bolstering prevention, incident reporting, and coordinated response, there remain notable gaps in adopting more proactive "active defense" tactics, including deliberate diversion of attackers to decoy systems (Divert) and strategic deception (Deceive).

This study examines the alignment between the EU's evolving cybersecurity mandates and the operational tactics essential for modern resilience. By highlighting both successes and gaps, the research underscores the need to refine regulatory guidance, ensuring that organizations can confidently employ the full spectrum of defensive measures, proactive as well as reactive, within a legal and ethical framework. In doing so, it contributes to an increasingly urgent discourse on shaping a defense architecture that effectively mitigates advanced threats while respecting fundamental rights and fostering collective security.

II. Methodology

This study employs a structured, multi-step qualitative methodology augmented by targeted quantitative insights to examine how key EU cybersecurity regulations, NIS2, the Digital Operational Resilience Act (DORA), the Cyber Resilience Act (CRA), the Cybersecurity Act (CSA), the Critical Infrastructure Directive (CID), and the Cyber Solidarity Act (CSoA), align with operational tactics for cyber resilience. The approach is designed to address both the legal-textual components of these instruments and their practical impact on improving cybersecurity postures across the EU. Specifically, the methodology unfolds through the following seven steps:

1. **Selection of Regulatory Instruments**: The first step was to select the primary EU regulations and directives most relevant to cybersecurity. NIS2, DORA, CRA, CSA, CID, and CSoA were chosen due to (a) their centrality in the EU's legislative agenda, (b) the broad range of sectors they cover (finance, critical infrastructure, ICT products, etc.), and (c) their influence on Member States' cybersecurity requirements. These six frameworks constitute the core of the EU's evolving cybersecurity landscape, justifying their inclusion over more specialized or national-level regulations.
2. **Data Collection and Coding**: Official legislative texts and related explanatory documents were collected from the Official Journal of the European Union and from publications by the European Union Agency for Cybersecurity (ENISA). Using a deductive coding approach, each article or clause in the legislative texts was examined for references, explicit or implicit, to any of the six high-level defensive tactics: Redirect, Obviate, Impede, Detect, Limit, and Expose. To capture finer detail, the subcategories (e.g., Divert, Deceive, Delay) were coded for explicit or inferred presence. This step ensured consistency through a standardized codebook of operational tactics applied across all regulatory texts.
3. **Qualitative Content Analysis**: A qualitative content analysis framework was then applied to interpret how each regulation addresses (or omits) specific tactics. Relevant articles were tagged and annotated to identify legal mandates,

recommended practices, and potential constraints, particularly regarding proactive or "active" defense measures. Where an article tangentially aligned with a tactic, the research team conducted further examination to determine whether it explicitly supported, discouraged, or remained neutral toward that tactic.

4. **Incorporation of Quantitative Indicators**: Although the study is primarily qualitative, quantitative indicators were integrated to gauge regulatory impact. For example, ENISA's "State of Cybersecurity in the Union" reports, sector-specific compliance rates (e.g., DORA's effect in the financial sector), and incident reporting metrics offered quantitative context. These statistics provided evidence of how the chosen regulations have tangibly influenced cybersecurity practices, lending additional credibility to the qualitative findings.
5. **Case Study Validation**: To illustrate real-world relevance and validate the coding outcomes, publicly documented cyber incidents (e.g., WannaCry, Colonial Pipeline, and Emotet takedowns) were referenced. These examples helped confirm whether the tactics inferred from the legislative texts have been, or could be, practically deployed in ongoing cyber defense measures.
6. **Comparative Assessment and Synthesis**: A cross-regulation comparison was conducted to highlight commonalities and gaps. Specifically, the analysis focused on whether advanced tactical subcategories (e.g., Divert, Deceive, Preempt) were explicitly addressed or conspicuously absent. Findings were synthesized into tables and summary matrices mapping each regulation to the relevant tactics, thereby revealing areas of robust coverage and unaddressed vulnerabilities.
7. **Limitations and Future Research**: While this methodology offers a systematic way to identify and categorize regulatory provisions, it does not measure the degree of real-world implementation, nor does it fully resolve legal or ethical ambiguities surrounding more proactive tactics. Future empirical work (e.g., interviews with national authorities, surveys of regulated entities) may expand upon these findings by assessing how, and whether, organizations operationalize these tactics under current EU law.

By integrating a structured coding framework, referencing quantitative impact metrics, and validating findings through documented cyber incidents, this methodology ensures that the analysis extends beyond a mere summary of legal texts. It offers a reasoned exploration of both the strengths and gaps in EU cybersecurity regulations, clarifying their alignment with a comprehensive set of operational tactics for modern cyber resilience.

III. Literature Review

The debate on the efficacy of offensive cyber strategies and the need to adopt resilience-focused approaches has been a recurring theme in specialized literature. Valeriano and Jensen [1], in their seminal work on The Myth of the Cyber Offense, question the widely held assumption that offensive cyber operations offer decisive strategic advantages. Their findings, based on incidents from 2000 to 2016, suggest that most cyber operations exhibit restraint, and that the deterrent effect of offensive strategies is limited. This study is a vital precedent as it highlights the significance of defensive resilience and intelligence sharing, elements aligned with the European Union's (EU) increasingly operational and regulatory push toward resilience rather than overt cyber retaliation.

In the same vein, Shackelford et al. [2] delve into the notion of "active defense" or hackback, comparing U.S. legislative attempts (e.g., the proposed Active Cyber Defense Certainty Act) with initiatives in China, Singapore, Thailand, Australia, and the G7. Although "hack back" faces substantial challenges due to possible escalation and legal complexities, policy discussions reveal growing support for giving private firms more proactive defensive capabilities. Such interest, however, necessitates a careful regulatory framework that

balances critical infrastructure protection and the risks of unintended cyber escalations.

From a legal standpoint, Bradbury [3] explores how governments, particularly the United States, design their cyber defenses and responses, addressing Fourth Amendment constraints and privacy laws through consent-based monitoring systems like EINSTEIN. He underscores the importance of executive discretion in an international context that lacks clear norms for cyber conflict, an observation that underscores the dynamic interplay between national security needs and individual liberties.

Moving to doctrinal and tactical considerations, Couretas [4] links cyber policy, doctrine, and tactics, techniques, and procedures (TTPs) to illustrate how different layers of guidance reinforce both defensive and offensive cyber operations. Complementing that perspective, Leventopoulos et al. [5] propose a framework for state-level responses to cyber-attacks, going beyond traditional incident response. Their structured chain of command, connecting real-time cyber sensors with decision-makers, supports escalation pathways from non-action to potential cyber or even kinetic measures, pushing the boundaries of current international norms yet deemed essential for national security deterrence.

The life cycle of offensive cyber capabilities is thoroughly dissected by DeSombre et al. [6], who characterize proliferation as a multi-layered process, encompassing vulnerability research, malware payload development, command-and-control structures, operational management, and ongoing training. By segmenting offensive cyber capability development into these stages, the authors illuminate critical policy levers for restricting illicit proliferation while acknowledging the concurrent need to foster innovation in cybersecurity research.

In the international legal sphere, the Tallinn Manual 2.0 [7] frames cyber operations through a broader lens that extends beyond purely technical classification. It highlights a continuum of state actions, ranging from preemptive to remedial, and underscores the significance of transparency in cyberspace engagements. This resonates with the EU's challenge of balancing the protection of critical networks and the safeguarding of fundamental rights [8–10].

In particular, González Fuster and Jasmontaite [8] trace the evolution of EU cybersecurity regulation, from the early 2013 Cybersecurity Strategy to the more holistic measures of the 2017 updates. Despite notable progress, they emphasize ongoing tensions regarding overlapping regulatory goals and actors' roles in ensuring compliance. Bederna and Rajnai [9] further reveal the complexities of the EU cybersecurity ecosystem, where interdependencies across numerous stakeholders highlight persistent gaps, especially involving eGovernment entities and smaller service providers, thus calling for more cohesive legislation.

At the national level, Jacuch [10] showcases how inconsistent implementation of EU directives undermines overall cyber resilience, using Poland as a case study. This aligns with the broader argument that national strategies must be harmonized to form a robust regional defense across the EU Digital Single Market.

Organizationally, literature points to the importance of embedding cybersecurity culture. Annarelli and Palombi [11] demonstrate how capabilities in digitalization, such as asset reconfiguration, environmental scanning, and improvisation, are crucial to sustaining cyber resilience from preparation to adaptation. Similarly, Neri et al. [12] show that, while technical measures like asset cataloging are often in place, many small and medium-sized enterprises (SMEs) lag behind in establishing a structured cybersecurity policy or fostering adequate awareness, thus undermining their capacity to withstand modern cyber threats.

Taken as a whole, the research underscores a marked shift toward resilience as the linchpin of contemporary cybersecurity. While some authors underscore moderation and well-framed active defense [1,2], others explore the legal foundations for stronger response measures [3–5]. The EU, caught at the intersection of these debates, has created directives and regulations that, though comprehensive, still struggle to integrate practical, operational tactics like deception or proactive diversion [8–10]. In parallel, the organizational perspective stresses the imperatives of cultivating awareness, training, and dynamic resource

management to ensure that resilience transcends mere prevention and enables continuity and effective recovery [11,12].

IV. Problem and Possible Solutions

The problem emerges from the gap between the robust preventive, detection, and collaborative measures mandated by EU directives, such as NIS2 , DORA, CRA, CSA, CID, and the Cyber Solidarity Act, and the operational tactics organizations need to effectively defend against increasingly sophisticated threats. While these regulations establish a strong baseline for resilience, they often do not include explicit guidance on more proactive or "active" approaches, such as the ability to divert attackers toward decoy resources or to deceive adversaries with misleading information. These omissions stem largely from legal and ethical concerns related to manipulating attackers, as well as the absence of clear regulatory language that would enable companies to adopt a more assertive defense without risking liability or violating other legal provisions. Consequently, critical sectors frequently opt for overly cautious strategies to avoid potential legal uncertainties.

Possible solutions focus on achieving a reasonable balance between heightened proactivity and existing legal and ethical obligations. First, creating complementary "soft-law" guidelines to accompany EU regulations could explicitly describe how to implement advanced tactics like redirection or deception. These guidelines should include proportionality standards, technical validation procedures, and a minimum level of transparency to prevent misuse. Second, supervised pilot programs led by agencies such as ENISA could empirically evaluate the effectiveness and impact of more advanced tactics in controlled environments, providing a legal framework for experimentation. Finally, public-private collaboration is central: sharing threat intelligence and experiences with active defense methods could help build trust, disseminate best practices, and mitigate risks related to innovation in cyber defense.

By strengthening the regulatory foundation while encouraging practical, ethically sound approaches that leverage the full spectrum of available tactics, both industry and public organizations would move toward a more robust cyber posture, one that effectively reduces vulnerabilities and is better equipped to anticipate the evolving digital threat landscape.

V. Operational tactics for cyber resilience

The foundation of cyber resilience lies in understanding and effectively implementing operational tactics that disrupt the adversary's actions throughout the cyberattack lifecycle. These tactics are encapsulated in six high-level effects: Redirect, Obviate, Impede, Detect, Limit, and Expose. While these terms provide a broad framework for describing defensive measures, their generality necessitates more specific subcategories to enable actionable and measurable outcomes for cyber defenders [13]. For example, Prevent and Preempt refine the scope of Obviate, while Contain, Curtail, Recover, and Expunge enhance the practical application of Limit. These tactical effects are not only pivotal for neutralizing specific adversary activities but also for increasing the cost, decreasing the benefit, or amplifying the risks faced by attackers across various stages of their campaigns [13].

By employing this terminology, defenders can assess how architectural choices, technological investments, and defensive measures collectively influence adversaries. These tactics provide both an operational framework for proactive defense and a pathway to achieving strategic cyber resilience objectives. They underscore a necessary shift in cybersecurity, from mere prevention to a holistic resilience model emphasizing adaptability, recovery, and sustained operations under adverse conditions. This chapter explores these tactics, illustrating their effectiveness in mitigating threats and maintaining the continuity of critical systems and services as illustrated in Fig. 1.

Operational tactics provide a comprehensive framework to counter cyber threats by targeting specific phases of the adversary's lifecycle. These tactics, along with their detailed subcategories, enable defenders to implement precise measures to disrupt, delay, and mitigate adversarial activities. The following Table I elaborates on each tactic and its respective subcategories, defining their roles and objectives within a cyber resilience strategy.

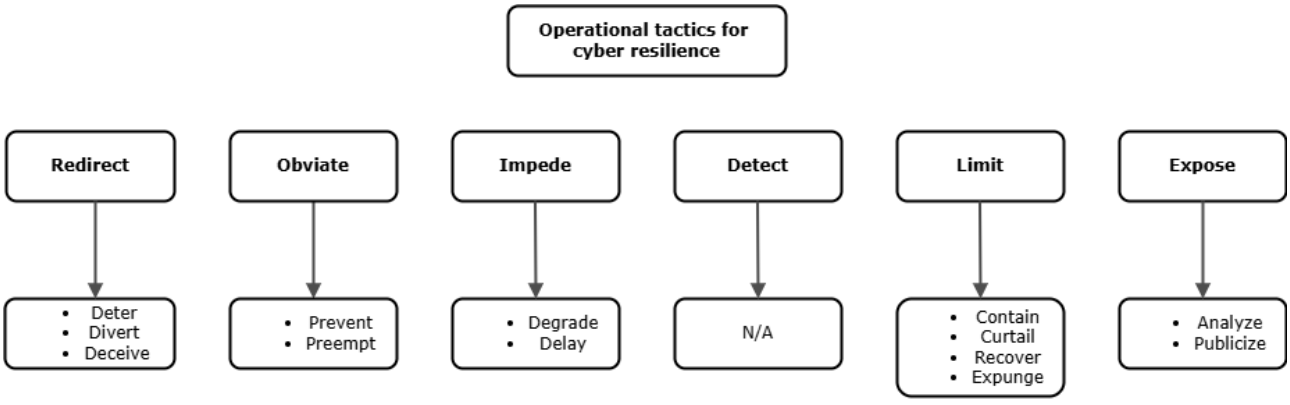

Fig. 1. Operational tactics for cyber resilience.

TABLE I
OPERATIONAL TACTICS FOR CYBER RESILIENCE.

Tactic	Subcategory	Definition	Objective
Redirect	Deter	Discourage adversaries from engaging in malicious activities by instilling fear (e.g., attribution) or doubt.	Stop adversary activities by increasing perceived risks or lowering the likelihood of success.
	Divert	Lead adversaries to redirect their activities to non-critical or decoy systems.	Waste adversary resources and protect vital systems by using honeynets or pre-selected targets.
	Deceive	Mislead adversaries by presenting false information about defended systems or capabilities.	Cause adversaries to rely on incorrect data, leading to wasted efforts or incorrect actions.
Obviate	Prevent	Ensure adversarial activities are ineffective or fail to achieve their goals.	Render attacks futile by using preventive controls like email filtering or Data Loss Prevention (DLP).
	Preempt	Act proactively to disrupt or disable adversarial resources before they can be used.	Deny adversaries the ability to act by destroying or making their resources inaccessible.
Impede	Degrade	Reduce the effectiveness of adversarial activities or the impact of their actions.	Limit the scope or severity of attacks through patching, configuration changes, or cryptographic protections.
	Delay	Increase the time required for adversaries to achieve their objectives.	Expose adversaries to higher detection risks and force them into inefficient attack methods.
Detect	N/A	Identify adversary activities or indicators of compromise in real time.	Enable rapid defensive responses to mitigate ongoing or imminent threats.
Limit	Contain	Restrict adversarial actions to a defined set of resources to minimize damage.	Isolate affected systems to prevent further spread or escalation of the attack.

Tactic	Subcategory	Definition	Objective
	Curtail	Limit the duration of adversarial activities.	Reduce the time during which adversarial actions impact systems or operations.
	Recover	Reverse the impacts of adversarial actions to restore normal operations.	Reinstate compromised systems using backups or redundant systems.
	Expunge	Permanently remove adversarial malware or corrupted data.	Eliminate threats by erasing malicious components and repairing compromised resources.
Expose	Analyze	Study adversarial actions, including their tactics, techniques, and procedures (TTPs).	Gain actionable intelligence to preempt or mitigate future adversarial actions.
	Publicize	Share threat intelligence and observations across organizations and sectors.	Strengthen collaborative defenses and diminish adversarial stealth through shared awareness.

In a scenario where a multinational corporation detects suspicious activity targeting its intellectual property, operational tactics offer a systematic way to counter the threat. By employing the high-level categories of Redirect, Obviate, Impede, Detect, Limit, and Expose, organizations can move beyond purely reactive responses and implement proactive, resilience-driven strategies to protect critical data.

Redirect (Deter, Divert, Deceive) involves misdirecting or misleading the adversary to reduce their likelihood of success. In this example, the corporation sets up a honeynet (an artificial environment designed to appear genuine) where an adversary believes they have accessed valuable intellectual property. By creating fabricated credentials (Deceive) and funneling attackers away from real systems (Divert), defenders waste the adversary's time and resources. This tactic ultimately deters future attacks by raising perceived risks and complicating adversarial efforts.

Obviate (Prevent, Preempt) focuses on ensuring that adversarial actions cannot take hold. Here, the organization implements robust access controls and multifactor authentication (Prevent), blocking unverified intruders at the outset. Frequent patching and vulnerability scans address potential security gaps in advance (Preempt), ensuring that adversaries cannot exploit uncorrected flaws. Together, these measures reduce the likelihood that malicious actors will penetrate critical systems in the first place.

Impede (Degrade, Delay) comes into play if an adversary manages to bypass initial defenses. By encrypting sensitive data (Degrade), the organization makes any stolen information less useful to attackers. Simultaneously, adaptive throttling (Delay) slows data extraction attempts, compelling adversaries to spend more time and resources, thereby increasing their exposure to detection. Meanwhile, Detect is achieved through real-time network monitoring and behavioral analytics that flag abnormal access patterns or data transfer volumes. Swift identification of suspicious activity allows defenders to intervene before significant damage occurs.

Upon confirming an intrusion, the Limit tactic contains and neutralizes adversarial effects. Contain isolates compromised systems to prevent lateral movement, while Curtail revokes unauthorized privileges to stop ongoing intrusions. Automated tools facilitate Recover by restoring or replacing compromised files and Expunge by eliminating malicious artifacts. The Expose tactic enhances defenses: defenders Analyze adversarial tactics in honeynets and Publicize indicators of compromise to partners or sector consortiums. This exchange of knowledge disrupts attacker secrecy

and reduces future risks. Together, these tactics mitigate immediate threats and bolster long-term cyber resilience in an evolving threat landscape.

A clear illustration of how these tactics manifest in real scenarios can be seen with Redirect, which comprises Deter, Divert, and Deceive. In the "Deter" subcategory, the conviction of Edwin Pena, sentenced to 10 years in prison for a VoIP hacking scheme, epitomizes how coordinated law enforcement action and clear attribution can substantially raise the perceived cost of cybercrime [14][15]. Meanwhile, the takedown of the GameOver Zeus botnet serves as a prime example of "Divert," where court orders rerouted infected computers from criminal servers to neutral, government-controlled servers, compelling adversaries to spend resources on non-critical assets [16]. The FBI's Operation Trojan Shield underscores "Deceive": adversaries were misled into trusting an FBI-controlled encrypted service, resulting in the interception of millions of messages and a large-scale law enforcement sweep [17].

Under Obviate, which encompasses Prevent and Preempt, standard best practices such as multifactor authentication, timely patching, and employee training exemplify "Prevent," proactively closing off key attack vectors before malicious actors gain a foothold. However, while the Paris Olympic Games' extensive cybersecurity measures prevented many disruptions, they mostly centered on sustaining resilience under attack rather than actively dismantling adversarial infrastructure, thereby stopping short of the more proactive "Preempt" approach [18].

Moving to Impede, which covers Degrade and Delay, Microsoft's release of the MS17-010 patch typifies "Degrade": organizations that rapidly applied this fix against SMB Server vulnerabilities directly diminished WannaCry's impact by restricting the ransomware's ability to exploit those flaws [19]. In SDN-IoT architectures, "Delay" tactics such as rate limiting and aggressive flow-table aging force adversaries to expend more resources over longer periods, creating heightened exposure to detection [20].

Across all phases, Detect remains pivotal. Continuous monitoring, anomaly-based detection, and intelligence-sharing platforms ensure that once adversaries initiate their moves, be it lateral traversal or data exfiltration, defenders can swiftly identify and respond.

Under Limit, which comprises Contain, Curtail, Recover, and Expunge, the Colonial Pipeline ransomware event highlights "Contain," as the company quickly isolated compromised IT systems and prevented further intrusion [21]. The WannaCry ransomware outbreak demonstrates "Curtail," where a researcher registering a hard-coded domain abruptly ended the malware's global rampage [22]. During the NotPetya attack, A.P. Møller–Maersk exemplified "Recover" by salvaging its entire Active Directory from a lone domain controller in Ghana, enabling the quick restoration of critical services [23]. Finally, "Expunge" was showcased in January 2021 when a coalition of law enforcement agencies eradicated Emotet by replacing its malicious payload on infected systems with a benign file, effectively severing command-and-control and removing the malware [24].

Lastly, Expose involves Analyze and Publicize. The SolarWinds compromise exemplifies "Analyze": dissecting its sophisticated supply chain infiltration provided insights into how attackers established prolonged stealth within high-value networks [25]. The WannaCry incident underscores "Publicize," as open sharing of threat intelligence, patches, and indicators of compromise sped up worldwide response and mitigation efforts, illustrating the value of collaborative transparency [26].

Together, these cases illustrate how each tactic, Redirect, Obviate, Impede, Detect, Limit, and Expose,l contributes to a resilient cybersecurity posture. Even if initial preventive measures fail, subsequent tactics continually erode adversarial momentum, forcing attackers to devote more resources under ever-increasing risk of detection and neutralization. Ultimately, this layered approach moves organizations from a static, prevention-only stance to an adaptive defense model, significantly reducing both the likelihood and impact of sophisticated cyberattacks.

VI. Legal And Ethical Perspectives

This chapter examines whether the provisions of key European Union cybersecurity regulations, namely the NIS2 Table III, CRA Table IV, DORA Table V, CSA Table VI, CID Table VII, and the CSoA

Table VIII, embody legal principles or "legal goods" aligned with specific operational tactics. By identifying and analyzing relevant articles within these legislative texts, the chapter evaluates their direct applicability to defensive maneuvers and demonstrates how aligning compliance with EU norms both strengthens cyber resilience and supports effective operational responses. Notably, the EU's cybersecurity legal framework was chosen as the primary point of reference owing to its demonstrable regulatory impact, which is substantiated by multiple quantitative indicators.

For instance, ENISA's 2024 Report on the State of Cybersecurity in the Union notes an overall EU Cybersecurity Index of 62.65 out of 100, with a narrow inter-member deviation of just 3.76 points, signaling a marked convergence in cybersecurity capabilities attributed to the Union's robust and cohesive legislative measures. Additionally, sector-specific case studies reveal that 55% of transport operators credit the previous NIS Directive with significantly driving their cybersecurity investments. These concrete metrics, together with the measurable improvements in incident reporting and preparedness since the adoption of instruments like the NIS2 Directive, the Cyber Resilience Act, and the Cyber Solidarity Act, underscore the practical efficacy of EU legislation in raising cybersecurity standards across the continent. Consequently, basing this study on EU regulations not only leverages a comprehensive array of horizontal and sector-specific rules but also draws on tangible evidence of their effectiveness in boosting cybersecurity resilience throughout the Union [27].

A. Network and Information Security Directive (NIS2)

EU NIS2 [28] covers a broad defensive scope but leaves certain sub-tactics unexplored:

Redirect (Deter, Divert, Deceive): Article 7 requires national cybersecurity strategies that deter adversaries via improved security practices and coordination. Article 24 encourages certified ICT products, raising adversaries' costs. Yet it does not explicitly address Divert (steering attackers to decoys) or Deceive (misleading adversaries), reflecting ethical and legal caution around entrapping or manipulating threat actors.

Obviate (Prevent, Preempt): Article 11(1)(b)(e)(f)(2) mandates robust staffing, secure facilities, and backup capabilities to neutralize threats proactively. Article 21(1) requires proportionate risk management, thereby helping to prevent incidents. However, Preempt (actively disabling adversarial resources before deployment) is absent, likely due to high attribution risks and potential cross-border legal conflicts.

Impede (Degrade, Delay): Article 21(1) fosters safeguards (e.g., patches, access controls) that degrade attack efficacy. Deliberate delay tactics are not stated, possibly due to liability concerns around prolonging adversary engagement.

Detect: Central under Article 11, which empowers CSIRTs to monitor, analyze, and swiftly detect threats. Article 11(3)(a)(e) emphasizes early scanning and real-time notification, spotlighting detection over adversary manipulation.

Limit (Contain, Curtail, Recover, Expunge): Article 11(3)(c) supports containment and swift recovery, but there is no direct mention of Curtail or Expunge. These subtactics often require specialized protocols, left to individual Member States' discretion.

Expose (Analyze, Publicize): Article 11(3)(b) encourages real-time intelligence sharing; Article 12 formalizes coordinated vulnerability disclosure. While these provisions foster situational awareness, naming or shaming adversaries is avoided, consistent with privacy norms and legal caution within the EU.

Overall, NIS2 stresses resilience, rapid response, and collaboration, leaving advanced sub-tactics, such as Divert, Deceive, Preempt, Delay, largely unaddressed.

B. Digital Operational Resilience Act (DORA)

DORA [29] focuses on risk management and incident preparedness across financial entities:

Redirect (Deter, Divert, Deceive): Articles 16(3) and 27 require strong ICT risk frameworks and threat-led penetration testing to deter attacks. Divert or Deceive are not explicitly mentioned,

in line with the EU's general reluctance to codify deceptive practices.

Obviate (Prevent, Preempt): Articles 7, 9, 11, 16, 17 emphasize early detection of vulnerabilities and proactive defense. Preempt, however, remains legally undefined, likely due to controversies around offensively targeting adversary infrastructure.

Impede (Degrade, Delay): Articles 9(1) and 9(4)(b) discuss network segmentation, which can degrade an attacker's lateral movement. Delay (intentionally slowing attackers) is implied in best practices (e.g., layered authentication) but not codified.

Detect: Articles 10, 15(c), and 16(1)(d) require continuous monitoring, ensuring threats are identified quickly.

Limit (Contain, Curtail, Recover, Expunge): Containment is found in Articles 9(4)(b) and 11(2)(b). Recovery measures (Articles 12, 15(f), 16(1)(f)) focus on backups and rapid restoration. Although Curtail and Expunge are indirectly referenced, DORA does not articulate specific protocols for removing attacker footholds.

Expose (Analyze, Publicize): Articles 1(1)(a)(ii)(iii), 13, 16(1)(h) advocate threat classification and transparency. Public disclosure of attacker information is less direct, reflecting privacy and liability concerns.

By centering on resilience, testing, and swift containment, DORA echoes the broader EU stance that advanced or deceptive tactics require greater legal clarity before adoption.

C. Cyber Resilience Act (CRA)

The Cyber Resilience Act [30] integrates market enforcement (e.g., CE marking) with cybersecurity requirements:

Redirect (Deter, Divert, Deceive): Articles 27, 28, 30, 53 deter through strict compliance and enforcement powers. Divert or Deceive remain out of scope to avoid blurring lines between legitimate consumer protection and potential entrapment.

Obviate (Prevent, Preempt): Multiple articles (4, 5, 6, 10, 12, 13, 19–22, 24, 32, 33, 57, and Annex I) promote risk management and "secure by design." Preempt, as a more offensive measure, is not addressed, consistent with the EU's concern about extraterritorial or unilateral cyber actions.

Impede (Degrade, Delay): Annex I(2)(i)(k) outlines functionality-limiting measures during compromise, but deliberate delay tactics are not mentioned. This may reflect the complexity of legislating partial engagement strategies.

Detect: Article 54 (continuous monitoring) and Annex I(2)(d) (real-time threat detection) specify robust detection mechanisms.

Limit (Contain, Curtail, Recover, Expunge): Annex I(2)(j) mentions containment; more detailed Curtail, Recover, or Expunge protocols are left to industry or sector-specific best practices.

Expose (Analyze, Publicize): Articles 14–17 and Annex I Part II(6)(7)(8) guide data analysis, reporting, and transparency but avoid actively publicizing attacker identities.

Ultimately, the CRA reinforces preventive product requirements and quick incident reporting, sidelining more assertive, ethically contentious tactics.

D. Cybersecurity Act (CSA)

The Cybersecurity Act (CSA) [31] formalizes cybersecurity certification and standardization in the EU:

Redirect (Deter, Divert, Deceive): Articles 8, 46, 52, 56 establish certification schemes that deter low-level threats. Divert and Deceive remain unaddressed, aligning with the EU's emphasis on transparency over subterfuge.

Obviate (Prevent, Preempt): Articles 10, 51, and 58 focus on promoting secure-by-design practices and raising public awareness. Preempt is missing, consistent with the EU's typical stance on refraining from endorsing offensive measures.

Impede (Degrade, Delay): The CSA implies that strong authentication and patching degrade attackers' capabilities, but it does not reference a formal strategy to delay adversaries.

Detect: Article 6(1)(c) tasks ENISA with improving detection across Member States, underscoring the EU's preference for collective defense and information sharing.

Limit (Contain, Curtail, Recover, Expunge): Article 6(1)(a) entrusts ENISA with assisting in incident response and recovery. Detailed sub-tactics (e.g., containing or curtailing intrusions) are not explicitly spelled out.

Expose (Analyze, Publicize): Articles 7(4)(c)(d), 9, and 11 encourage data pooling, research collaboration, and vulnerability analysis, but not active deception or naming adversaries.

Hence, the CSA bolsters cross-border certification and information-sharing but omits offensive or misleading strategies.

E. Critical Infrastructure Directive (CID)

The Critical Entities Resilience Directive [32] targets physical and cyber resilience for vital sectors:

Redirect (Deter, Divert, Deceive): Article 14 requires background checks to deter insider threats. Divert and Deceive remain absent, possibly due to strict oversight of critical sectors and avoidance of potential legal pitfalls.

Obviate (Prevent, Preempt): Articles 5, 10, 13(1)(a)(b)(e)(f) emphasize risk assessments and security controls. Preempt is missing, reflecting the legal complexity of proactively disabling threats that may lie outside national boundaries.

Impede (Degrade, Delay): Article 13 addresses resilience but lacks instructions for systematically degrading or slowing attackers.

Detect: Article 15 promotes timely notifications and cross-border coordination, supporting a rapid detection model.

Limit (Contain, Curtail, Recover, Expunge): Article 13(1)(c)(d) covers crisis management and business continuity, focusing on post-incident recovery. The Directive does not detail how to isolate or curtail adversaries during an attack.

Expose (Analyze, Publicize): Article 19 endorses information sharing to improve resilience but avoids explicit adversary analysis or naming.

Hence, the CID prioritizes preventive resilience and rapid responses in critical sectors without endorsing advanced adversary manipulation.

F. Cyber Solidarity Act (CSoA)

The Cyber Solidarity Act [33] seeks to establish collaborative EU mechanisms:

Redirect (Deter, Divert, Deceive): Article 12's EU Cybersecurity Reserve strengthens deterrence through heightened readiness but omits explicit mention of decoys or deception.

Obviate (Prevent, Preempt): Articles 3(2)(c), 8, 10, 11 focus on robust preventive testing. As with other EU laws, Preempt is not codified.

Impede (Degrade, Delay): Article 13 discusses resilience measures but provides no framework for deliberate degradation or time-buying tactics.

Detect: Articles 3(2)(d) and 4(1) direct the creation of Security Operations Centers for improved situational awareness and quick detection.

Limit (Contain, Curtail, Recover, Expunge): Article 9 supports large-scale incident recovery and removal of malicious artifacts. Contain and Curtail remain unspecified, consistent with a focus on restoring normalcy rather than confronting attackers.

Expose (Analyze, Publicize): Articles 14, 3(2)(a), 6, 7 advance threat analysis and data sharing across borders. Public naming or deception remains outside the legal scope.

While the CSoA underscores coordinated, collective defense, it avoids more assertive or deceptive tactics, reaffirming the EU's traditional stance on legal certainty and proportionate cyber operations.

G. Comparative Analysis of Global Cybersecurity Frameworks: The EU versus the United States

In addition to the EU's predominantly defensive and harmonized approach, comparing it with the United States illuminates broader regulatory trends. As shown in Table II, the EU aims for a top–down, rights-focused model that integrates cybersecurity with data protection and uniform enforcement. By contrast, the U.S. adopts a more fragmented, sector-specific regime, pairing reactive enforcement (e.g., through agencies like the FTC and SEC) with explicit statutory authority for offensive cyber operations, particularly under national security mandates.

Overall, both frameworks pursue robust cybersecurity but diverge in their policy philosophies. The EU emphasizes legal certainty, uniform protection of civil liberties, and harmonized defenses, whereas the U.S. legal environment grants more room for offensive measures at the federal level. Understanding these distinctions underscores how the EU's advanced sub-tactics, Divert, Deceive, Preempt, Delay, remain legally and ethically

TABLE II
CYBERSECURITY FRAMEWORKS: THE EU VERSUS THE UNITED STATES [10, 34]

Dimension	European Union	United States
Regulatory Structure	Harmonized supranational directives/regulations (e.g., NIS, GDPR, Cybersecurity Act), mandating uniform security standards.	Fragmented mix of federal statutes and state laws with sector-specific, market-driven approaches.
Focus on Fundamental Rights	Emphasizes protecting fundamental rights, embedding data protection principles into cybersecurity mandates.	Less prescriptive on privacy; focuses on safeguarding critical infrastructure and commercial interests.
Defensive Measures	Comprehensive, mandatory incident reporting and coordinated responses among Member States.	Defensive measures largely guided by voluntary standards (e.g., NIST Framework) and selective enforcement actions (FTC, SEC).
Offensive Cyber Capabilities	Primarily defensive; does not explicitly authorize offensive cyber operations, reflecting EU legal constraints and civil liberties concerns.	Explicitly permits offensive cyber actions for national security, military, and intelligence purposes under established legal frameworks.
Enforcement Mechanisms	Centralized oversight by EU institutions (e.g., ENISA) and national authorities, ensuring a level of vertical consistency.	Decentralized enforcement by multiple agencies (FBI, FTC, SEC), leading to variability in regulatory outcomes across states.
Global Coordination	Seeks cohesive international cybersecurity policies aligned with EU values; cooperates with NATO and other multilateral entities.	Operates often unilaterally or bilaterally, although recent initiatives indicate growing international cooperation.

constrained, even as the U.S. can more readily integrate them under national security doctrines.

On the other hand, EU cybersecurity frameworks, such as NIS2, DORA, CRA, CSA, CID, and the Cyber Solidarity Act, primarily focus on establishing legally binding requirements that often leave the explicit mapping to operational tactics at the discretion of individual organizations. In contrast, non-EU cybersecurity models offer a more flexible, risk-based approach that enables entities to tailor security strategies to specific threat environments and operational needs.

For instance, the NIST Cybersecurity Framework (CSF) 2.0 [35] is organized into six core functions (Govern, Identify, Protect, Detect, Respond, and Recover). This structure promotes continuous improvement and integration with enterprise risk management processes, thereby allowing an organization to prioritize relevant controls (including, in theory, deceptive measures or partial preemptive actions). Similarly, ISO/IEC 27001:2022 [36] offers a robust framework for establishing, implementing, and continually improving an Information Security Management System (ISMS), supporting systematic risk assessment and treatment. Complementing this, ISO/IEC 27002:2022 [37] provides detailed guidance on selecting and implementing security controls that can be aligned

with specific operational tactics—filling the gap between high-level legal mandates and practical cybersecurity measures.

By contrast, EU regulations often prescribe minimum common standards but do not necessarily address advanced tactics, like Divert or Deceive, within statutory texts. Consequently, organizations seeking more proactive or deceptive defenses can look to risk-based frameworks (e.g., NIST CSF, ISO/IEC 27001, ISO/IEC 27002) to supplement compliance with EU law, provided they navigate potential issues under General Data Protection Regulation (GDPR) and other data protection regulations.

H. Addressing Regulatory Gaps and Strengthening Cyber Resilience

The analysis of key EU cybersecurity regulations (NIS2, DORA, CRA, CSA, CID, and CSoA) reveals a consistent pattern: while these frameworks provide strong coverage of preventive, reactive, and collaborative security measures, they exhibit significant gaps in addressing advanced "active" defense tactics such as Divert, Deceive, and Preempt. These omissions stem from a complex interplay of legal, ethical, policy, and operational factors that reflect the EU's cautious approach to cybersecurity regulation.

From a legal and ethical perspective, the absence of provisions for active defense tactics can be attributed to concerns about potential conflicts with fundamental data protection principles under the GDPR and other privacy frameworks. Deceptive or preemptive operations raise difficult questions about proportionality and accountability, particularly when they involve manipulating adversary behavior or taking action against infrastructure that may cross jurisdictional boundaries. The risk of violating laws in the attacker's jurisdiction creates additional liability concerns for defenders, discouraging the adoption of more aggressive tactics.

At the policy level, the EU's regulatory approach prioritizes harmonized defense standards and risk-averse strategies over more confrontational measures. This reflects a deliberate choice to focus on establishing baseline security requirements and resilience-building rather than authorizing direct engagement with adversaries. The preference for predictable, proportional responses aligns with the EU's broader legal tradition but may leave organizations without clear guidance when facing sophisticated threats that demand more proactive defense measures.

Operational challenges further complicate the integration of active defense tactics into regulatory frameworks. Effective preemption requires reliable attribution of malicious actors - a notoriously difficult task in cyberspace. while techniques like deception demand specialized expertise and careful implementation to avoid unintended consequences. The diverse needs of different sectors (finance, healthcare, energy, etc.) make blanket mandates for advanced tactics impractical, suggesting that any future regulatory developments would need to accommodate sector-specific requirements.

Addressing these gaps will require balanced solutions that reconcile security needs with ethical and legal constraints. Potential approaches include controlled pilot programs under ENISA supervision to test active defense measures within strict boundaries, clearer legal definitions of permissible tactics to reduce uncertainty, and enhanced public-private collaboration to share threat intelligence. The EU might also consider iterative updates to existing regulations or soft-law approaches like voluntary guidelines that allow flexibility while mitigating risks. Any move toward authorizing active defense would need to incorporate robust oversight mechanisms, strict proportionality requirements, and cross-border coordination to maintain alignment with the EU's rights-based legal tradition and international obligations.

The current regulatory gaps highlight a fundamental tension in cybersecurity policy between the need for more proactive defense capabilities and the preservation of legal and ethical safeguards. While the EU's cautious approach ensures stability and protects fundamental rights, it may need to evolve to address the growing sophistication of cyber threats. Future policy developments will likely need to strike a careful balance between enabling effective defense and maintaining the EU's commitment to proportionality, accountability, and harmonized standards across member states.

VII. Results and Discussion

The comparative analysis of NIS2, DORA, CRA, CSA, CID, and the CSoA reveals a clear emphasis on prevention, detection, and coordinated response, aligning well with tactics such as Prevent, Detect, and elements of Limit (particularly containment and recovery). Across these frameworks, there is evident progress in mandating robust cyber risk management, incident reporting, and collaboration among stakeholders, key pillars of a resilience-based approach. For example, provisions in DORA on continuous monitoring and testing, or NIS2's focus on early threat detection, show strong support for Detect. Likewise, requirements for incident response in both NIS2 and the Cyber Solidarity Act effectively address Limit, mandating containment and recovery protocols that minimize the impact of attacks on essential services.

However, the results also highlight notable gaps in more advanced or "active" defensive tactics, such as Divert (guiding attackers to decoy systems), Deceive (deliberate misdirection through false information), and Preempt (disabling adversarial resources prior to an attack). None of the six EU instruments studied explicitly address these subcategories. The absence of direct references could be attributed to legal concerns around entrapment or liability, as well as an overarching regulatory priority to ensure compliance and transparency over potential manipulation of attackers. Yet these gaps are significant in practice: many sophisticated threat actors are deterred less by passive defensive measures and more by tactics that raise their operational costs or undermine confidence in their methods. Not incorporating these tactics into regulation may, therefore, limit the degree of proactive security organizations can confidently adopt, especially in highly regulated sectors that require explicit legal backing for more assertive measures.

Another limitation concerns Delay, which might be employed to prolong adversaries' exposure, thus increasing the chances of detection and thorough response. Despite references to network segmentation and layered authentication in instruments like NIS2 or DORA, measures that could inadvertently delay attackers, none of these frameworks clearly encourage strategies to deliberately slow malicious activities. This gap underscores the EU's cautious stance on deliberately engaging or interacting with an adversary beyond standard preventive controls.

From a broader perspective, these findings illustrate a tension between the EU's normative emphasis on risk management and the evolving requirement for organizations to adopt more flexible, adaptive defenses. While the analyzed directives and regulations have significantly raised baseline security standards, indicated by strengthened incident reporting obligations, common cybersecurity practices, and more cohesive cross-border cooperation, organizations seeking robust resilience may need additional guidance on implementing or even testing advanced tactics. In this sense, the EU legislative environment encourages collective defense and information sharing, yet remains conservative in codifying more assertive measures that venture into potential legal and ethical gray areas.

In light of these observations, two avenues emerge for enhancing EU regulatory frameworks. First, publishing supplemental guidelines or best practices could clarify the permissible scope of tactics like Divert or Deceive, establishing parameters for lawful experimentation with active defense under carefully defined conditions. Second, pilot programs under agencies like ENISA could systematically assess the ethical, operational, and legal dimensions of these advanced tactics, informing future updates to regulations. By gradually integrating these more proactive strategies, the EU can further align its cybersecurity model with resilience imperatives without compromising its core values of proportionality and respect for fundamental rights.

Overall, the results underscore that although EU cybersecurity regulations thoroughly address foundational resilience components, they leave room for improvement in codifying or supporting active defensive measures. Addressing these gaps could bolster both the strategic and tactical layers of defense, helping organizations anticipate and counter sophisticated threats while remaining

legally compliant within the EU's complex regulatory environment.

VIII. Limitations and Future Research

A key limitation of this study lies in its focus on six European Union frameworks, NIS2, DORA, CRA, CSA, CID, and the Cyber Solidarity Act, as the primary basis for qualitative analysis. While these regulations represent major instruments influencing EU cybersecurity policy, they may not capture the full spectrum of national transpositions or additional sector-specific guidelines within Member States. Consequently, local adaptations or supplementary measures could alter the degree to which certain tactical subcategories (such as Divert or Deceive) might be implicitly supported in practice.

Another limitation arises from the interpretive nature of the qualitative mapping. Assigning regulatory provisions to specific tactics, particularly subcategories of more proactive measures like Preempt or Delay, can involve subjective judgments. Given that these regulations seldom use tactical language, there is room for varying interpretations about the scope or intent of each article. Additionally, the legal and ethical complexities surrounding active defense strategies were beyond the purview of this research, restricting the discussion to a high-level evaluation rather than a granular legal analysis of, for instance, the boundaries of acceptable deception under EU law.

Regarding future research, several directions emerge. First, a more detailed legal-ethical assessment would shed light on whether and how tactics that interact directly with attackers could be integrated without contravening fundamental rights and established legal principles within the EU. This could involve case studies where controlled deception or targeted diversion have been tested in alignment with GDPR and other regulatory standards. Second, empirical inquiries into how specific organizations or sectors implement (or avoid) these less-explored tactics would provide granular insights into real-world adoption barriers, whether technical, legal, or cultural. Finally, comparing outcomes across different jurisdictions, such as a direct comparison of active defense adoption in the EU versus countries with more permissive legal frameworks for cyber operations, could further illustrate the role of legal structures in shaping defensive innovation. By deepening the knowledge on these aspects, future research can contribute to shaping a more adaptive, ethically grounded, and strategically cohesive cyber resilience model for the EU and beyond.

IX. Conclusion

Cybersecurity practices are undergoing a paradigm shift from a purely preventive stance to a more holistic resilience-focused model. While foundational measures, firewalls, access controls, and threat monitoring, remain indispensable, adversaries continue to evolve and exploit gaps in static defenses. The operational tactics framework examined in this study, Redirect, Obviate, Impede, Detect, Limit, and Expose, demonstrates how organizations can systematically counter sophisticated attacks across the entire threat lifecycle. By integrating proactive subcategories such as Divert or Deceive, defenders can meaningfully disrupt adversaries' strategies, raise operational costs for attackers, and reinforce organizational resilience.

A review of key EU regulations (NIS2, DORA, CRA, CSA, CID, and the Cyber Solidarity Act) highlights notable advancements in cybersecurity mandates, including robust risk management obligations, cross-border cooperation mechanisms, and incident reporting requirements. However, the absence of explicit support for more active tactics, particularly Divert, Deceive, Preempt, and Delay, points to an ongoing tension between the need for heightened cyber resilience and concerns over potential legal and ethical liabilities. This shortfall restricts the implementation of defensive techniques that could better anticipate and hinder advanced threats.

Bridging these regulatory gaps will require a concerted effort. Complementary guidelines, supervised pilot programs, and expanded public-private collaboration can clarify the scope and best practices for implementing advanced tactics within a responsible legal and ethical framework. By embedding these measures into EU-level policies, lawmakers and industry stakeholders can

foster a robust defense architecture that not only meets compliance obligations but also addresses the increasingly complex nature of modern cyberattacks. Ultimately, adopting a more comprehensive and adaptive tactical approach is paramount for safeguarding critical infrastructure, ensuring business continuity, and reinforcing trust in Europe's digital ecosystem.

Conflict of Interest

Author declares that they have no conflict of interest

FUNDING

The author of this article did not receive any particular grant from any public, commercial, or not-for-profit funding agency.

References

[1] B. Valeriano and B. Jensen, "The Myth of the Cyber Offense: The Case for Restraint," Cato Institute Policy Analysis, Washington, DC, USA, 2019. [Online]. Available: https://www.cato.org/policy-analysis/myth-cyber-offense-case-restraint

[2] S. Shackelford, A. Kastelic, S. Chraghchi, and B. Carroll, "Rethinkin Active Defense: A Comparative Analysis of Proactive ybersecurity Policymaking" Univ. Pa. J. Int'l L., vol. 41, no. 2, pp. 377-427, 2019. [Online]. Available: https://scholarship.law.upenn.edu/jil/vol41/iss2/3/

[3] S. Bradbury, "The Developing Legal Framework for Defensive and Offensive Cyber Operations," Harv. Natl. Secur. J., vol. 2, pp. 1-23, 2011. [Online]. Available: https://harvardnsj.org/wp-content/uploads/2011/02/Vol-2-Bradbury.pdf

[4] J. M. Couretas, "Cyber Policy, Doctrine, and Tactics, Techniques, and Procedures (TTPs)," in An Introduction to Cyber Analysis and Targeting, Cham, Switzerland: Springer, 2022, ch. 2. doi: 10.1007/978-3-030-88559-5_2

[5] S. Leventopoulos, K. Pipyros, and D. Gritzalis, "Retaliating against cyber-attacks: A decision-taking framework for policy-makers and enforcers of international and cybersecurity law," Int. Cybersecur. Law Rev., vol. 5, pp. 237–262, 2024. DOI: 10.1365/s43439-024-00113-5

[6] W. DeSombre, J. Cohen, A. De la Garza, J. Matis, and T. Porter, "A Primer on the Proliferation of Offensive Cyber Capabilities," Eindhoven Univ. Technol., Eindhoven, Netherlands, 2021. [Online]. Available: https://research.tue.nl/en/publications/a-primer-on-the-proliferation-of-offensive-cyber-capabilities

[7] M. N. Schmitt, Ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd ed., Cambridge, UK: Cambridge Univ. Press, 2017, pp.1–598, DOI: 10.1017/9781316822524

[8] G. G. Fuster and L. Jasmontaite, "Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights," in The Ethics of Cybersecurity, 1st ed., M. Christen, B. Gordijn, and M. Loi, Eds., Cham, Switzerland: Springer, 2020, ch. 5, pp. 1–46, DOI: 10.1007/978-3-030-29053-5_5

[9] L. Bederna and Z. Rajnai, "Analysis of the cybersecurity ecosystem in the European Union," Int. Cybersecur. Law Rev., no. 3, pp. 35–49, 2022, DOI: 10.1365/s43439-022-00048-9

[10] P. Jacuch, "Comparative analysis of cybersecurity strategies. European Union strategy and policies. Polish and selected countries strategies," Online J. Model. New Europe, no. 37, pp. 102–120, 2021DOI: 10.24193/OJMNE.2021.37.06

[11] A. Annarelli and G. Palombi, "Digitalization Capabilities and Sustainable Cyber Resilience: A Conceptual Framework," Sustainability, vol. 13, no. 23, p. 13065, 2021, DOI: 10.3390/su132313065

[12] A. Neri, F. Niccolini, and F. Martino, "Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment," Inf. Comput. Secur., vol. 32, no. 1, pp. 38–52, 2024, DOI: 10.1108/ICS-05-2023-0084

[13] D. Bodeau and R. Graubart, "Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment," MITRE Corp., Bedford, MA, USA, Tech. Rep. MTR 130432, Nov. 2013. [Online]. Availabl e: https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf [Accessed: Jan. 10, 2025].

[14] R. McMillan, "Man Gets 10 Years for VoIP Hacking," PCWorld, Sep. 24, 2010. [Online]. Available: https://www.pcworld.com/article/503431/article-2843.html.

[15] European Commission, Proposal for a Council Recommendation for an EU Blueprint on Cybersecurity Crisis Management, COM(2025) 66 final, Brussels, Belgium, Feb. 24, 2025. [Online]. Available: https://ec.europa.eu/newsroom/dae/redirection/document/113086.

[16] Federal Bureau of Investigation (FBI), "GameOver Zeus Botnet Disrupted: Collaborative Effort Among International Partners," FBI News, Jun. 2, 2014, updated

Jul. 11, 2014. [Online]. Available: https://www.fbi.gov/news/stories/gameover-zeus-botnet-disrupted.

[17] U.S. Department of Justice, "FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown," U.S. Attorney's Office, Southern District of California, Jun. 8, 2021. [Online]. Available: https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive.

[18] World Economic Forum, Global Cybersecurity Outlook 2025: Insight Report. Geneva, Switzerland: WEF, Jan. 2025. [Online]. Available: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.

[19] Microsoft Security Response Center, "Security Update for Microsoft Windows SMB Server (4013389)," Microsoft Security Bulletin MS17-010 - Critical, ver. 1.0, Mar. 14, 2017. [Online]. Available: https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010.

[20] C. Singh and A. K. Jain, "A comprehensive survey on DDoS attacks detection & mitigation in SDN-IoT network," e-Prime, Adv. Electr. Eng., Electron. Energy, vol. 8, p. 100543, Jun. 2024, DOI: 10.1016/j.prime.2024.100543.

[21] S. M. Kerner, "Colonial Pipeline hack explained: Everything you need to know," TechTarget, Apr. 26, 2022. [Online]. Available: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

[22] N. Khomami and O. Solon, "'Accidental hero' halts ransomware attack and warns: this is not over," The Guardian, May 13, 2017. [Online]. Available: https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack.

[23] S. Steinberg, A. Stepan, and K. Neary, NotPetya: A Columbia University Case Study, Rep. SIPA-21-022.1, Picker Center Digital Education Group, Columbia Univ., New York, NY, USA, 2021. [Online]. Available: https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf.

[24] U.S. Department of Justice, "Emotet Botnet Disrupted in International Cyber Operation," Office of Public Affairs, Jan. 28, 2021. [Online]. Available: https://www.justice.gov/archives/opa/pr/emotet-botnet-disrupted-international-cyber-operation.

[25] S. Oladimeji and S. M. Kerner, "SolarWinds hack explained: Everything you need to know," TechTarget, Nov. 3, 2023. [Online]. Available: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

[26] S. M. Khasru, "WannaCry shows that businesses and governments must cooperate," World Economic Forum, Jun. 1, 2017. [Online]. Available: https://www.weforum.org/stories/2017/06/wannacry-exposes-need-for-better-public-private-cooperation-in-the-cyber-space.

[27] European Union Agency for Cybersecurity (ENISA), "2024 Report on the State of Cybersecurity in the Union," Dec. 2024. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf.

[28] European Parliament and Council of the European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)," Official Journal of the European Union, vol. L 333, pp. 80-152, Dec. 2022. [Online]. Available: http://data.europa.eu/eli/dir/2022/2555/oj

[29] European Parliament and Council of the European Union, "Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance)," Official Journal of the European Union, vol. L 333, pp. 1-79, Dec. 2022. [Online]. Available: http://data.europa.eu/eli/reg/2022/2554/oj

[30] European Parliament and Council of the European Union, "Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)," Official Journal of the European Union, vol. L 2847, Nov. 2024. [Online]. Available: http://data.europa.eu/eli/reg/2024/2847/oj

[31] European Parliament and Council of the European Union, "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and

on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)," Official Journal of the European Union, vol. L 151, pp. 15-69, Jun. 2019. [Online]. Available: http://data.europa.eu/eli/reg/2019/881/oj

[32] European Parliament and Council of the European Union, "Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)," Official Journal of the European Union, vol. L 333, pp. 164-198, Dec. 2022. [Online]. Available: http://data.europa.eu/eli/dir/2022/2557/oj

[33] European Parliament and Council of the European Union, "Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)," Official Journal of the European Union, vol. L 2025/38, pp. 1-45, Jan. 2025. [Online]. Available: http://data.europa.eu/eli/reg/2025/38/oj

[34] J. X. Dempsey and J. P. Carlin, Cybersecurity Law Fundamentals, 2nd ed. Portsmouth, NH, USA: IAPP, 2024.

[35] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," NIST Cybersecurity White Paper, CSWP 29, Feb. 26, 2024. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.29

[36] ISO/IEC, "Information security, cybersecurity and privacy protection - Information security management systems - Requirements," ISO/IEC 27001: 2022, Oct. 2022.

[37] ISO/IEC, "Information security, cybersecurity and privacy protection - Information security controls," ISO/IEC 27002: 2022, 2022.

Appendixes

Appendix A

Tactical Objectives and Regulatory Measures Under the Network and Information Security Directive (NIS2).

TABLE III
A. TACTICAL OBJECTIVES AND REGULATORY MEASURES UNDER THE NIS2.

Tactic	Subcategory	Articles	Explanation
Redirect	Deter	Articles 7, 24	Article 7 mandates national cybersecurity strategies promoting deterrence through public awareness campaigns, honeynets, and decoy mechanisms. Article 24 supports deterrence by requiring certified ICT products to raise the cost and complexity for attackers.
	Divert	None	While not explicitly covered, diverting adversaries to alternate targets could be implemented through discretionary measures at the Member State or entity level.
	Deceive	None	No specific regulations on deception techniques like false information or systems; entities may apply such strategies independently.
Obviate	Prevent	Articles 11 (1)(b)(e)(f)(2), 21(1)	Article 11 requires secure facilities, staffing, and redundancy for CSIRTs. Article 21 enforces proportional risk-management measures for essential entities to minimize vulnerabilities.

Tactic	Subcategory	Articles	Explanation
	Preempt	None	The directive does not directly cover preemptive actions, which involve neutralizing threats before they materialize.
Impede	Degrade	Article 21 (1)	Article 21 promotes technical and organizational measures, like multifactor authentication and regular updates, to degrade attack effectiveness.
	Delay	None	No explicit focus on delaying adversarial actions to extend detection opportunities or operational timelines.
Detect	N/A	Articles 11 (3) (a) (e)	Article 11 requires CSIRTs to monitor cyber threats and vulnerabilities, conduct real-time scans, and proactively detect issues in network systems.
Limit	Contain	Article 11 (3) (c)	CSIRTs respond to incidents, limiting their scope and duration while aiding affected entities.
	Curtail	Article 11 (3) (c)	Similar to containment, focusing on restricting adversarial activities during incidents.
	Recover	Article 11 (3) (c)	Includes recovery actions like restoring services, eliminating malware, and utilizing backups to minimize disruptions.
	Expunge	Article 11 (3) (c)	Emphasizes removing adversarial traces such as malware and compromised data from affected systems.
Expose	*Analyze*	Articles 11 (3) (b), 12, 18, 23, 30	Outline key analytical tactics for cybersecurity. These include early warnings, coordinated vulnerability disclosure, regular risk assessments, and incident reporting. They emphasize proactive data sharing, collaboration among CSIRTs, and robust incident documentation to enhance detection and response across borders.
	Publicize	Articles 1 (2) (b) (c), 2 (13), 9(4) (5), 10 (3)(4)(7), 11(3)(h), 13(5), 14, 15, 16, 29.	Focus on publicizing cybersecurity information. They mandate secure information-sharing frameworks, transparency in risk communication, and cross-border collaboration. These provisions ensure critical entities and stakeholders are informed about risks, vulnerabilities, and mitigation strategies through structured cooperation and secure communication channels.

Appendix B

Tactical Objectives and Regulatory Measures Under the Digital Operational Resilience Act (DORA).

TABLE IV
A. TACTICAL OBJECTIVES AND REGULATORY MEASURES UNDER THE DORA.

Tactic	Subcategory	Articles	Explanation
Redirect	Deter	Articles 16(3), 27	Article 16(3) mandates ICT risk management frameworks to enhance resilience and mitigate risks. Article 27 requires Threat-Led Penetration Testing (TLPT) to simulate real-world attacks and improve system defenses.
	Divert	None	DORA does not explicitly address diverting adversaries to less critical targets; such strategies could be adopted at the discretion of individual entities.
	Deceive	None	Deceptive tactics like using false information or honeypots are not covered by DORA, leaving this as a potential area for further development.
Obviate	Prevent	Articles 7, 9(1)(3)(4), 11(6)(a)(b), 16(1)(b)(g), 17, 24, 25, 26	Articles focus on robust ICT systems, regular testing, and risk-based management practices to neutralize threats before they materialize.
	Preempt	Article 12(3)	Mandates segregated backup systems to prevent exploitation and ensure timely recovery, aligning with preemptive measures.
Impede	Degrade	Articles 9 (1)(4)(b), 11 (2)(b), 12(1)(a)(3), 16 (1) (c)	Articles address reducing attackers' effectiveness through measures like network segmentation, automated isolation mechanisms, and robust backup strategies.
	Delay	Articles 9 (4)(b), 12 (3)	Articles support slowing adversaries through automated mechanisms and segregated ICT systems to delay and impede attacks.
Detect	N/A	Articles 10, 15(c), 16(1)(d), 17	Articles mandate mechanisms for real-time detection of anomalies, detailed incident management processes, and multi-layered monitoring controls.
Limit	Contain	Articles 6(4), 9(4)(b), 11(2)(b), 12(5)	Articles focus on containment strategies such as network segmentation, secondary processing sites, and ICT continuity plans to limit attack spread.
	Curtail	Articles 11(2)(b), 15(b)(c)	Articles emphasize restricting damage through access control, tailored response measures, and robust containment protocols.

Tactic	Subcategory	Articles	Explanation
	Recover	Articles 11(2)(b)(3), 12(1)(b)(2)(4)(5), 15(f), 16(1)(f)	Articles highlight restoration measures, backup activation, and ensuring ICT capacity redundancy to recover swiftly from incidents.
	Expunge	Articles 12(2)(7), 15(f)	Articles address removing malicious artifacts and restoring data integrity after incidents to expunge adversarial traces.
Expose	Analyze	Articles 1(1)(a)(ii)(iii), 11(2)(e), 13, 16(1)(h), 18, 19, 48	Articles focus on post-incident reviews, vulnerability analysis, and integrating findings into risk management frameworks for continuous improvement.
	Publicize	Articles 1(1)(a)(v), 14, 44, 45	Articles mandate responsible disclosure, fostering collaboration, and establishing communication protocols to raise awareness of threats and vulnerabilities.

Appendix C

Tactical Objectives and Regulatory Measures Under the Cyber Resilience Act (CRA).

TABLE V
A. Tactical Objectives and Regulatory Measures Under the CRA.

Tactic	Subcategory	Articles	Explanation
Redirect	Deter	Articles 27, 28, 30, 53	Articles ensure that products meet harmonized standards and have conformity procedures, reinforcing deterrence by establishing robust cybersecurity baselines.
	Divert	None	No specific regulations are mentioned for diverting adversaries. Measures might be discretionary at Member State levels.
	Deceive	None	Deceptive tactics, such as using false information or systems, are not addressed within the regulatory framework.
Obviate	Prevent	Articles 4, 5, 6, 10, 12, 13, 19, 20, 21, 22, 24, 32, 33, 57, ANNEX I	These provisions mandate proactive risk management and secure configurations to prevent incidents. They also ensure manufacturers integrate robust security measures during product development.
	Preempt	ANNEX I (2)(h)	Preemptive actions include maintaining essential functions during incidents, supported by resilience and mitigation measures like protection from denial-of-service attacks.

Tactic	Subcategory	Articles	Explanation
Impede	Degrade	ANNEX I (2)(i)(k)	Provisions require minimizing the negative impact of compromised systems and reducing incident severity through exploitation mitigation techniques.
	Delay	None	No explicit provisions focus on delaying adversarial actions to increase response times or detection opportunities.
Detect	N/A	Article 54, 56, ANNEX I (2)(d)	Articles mandate real-time monitoring and reporting mechanisms, ensuring timely identification and response to emerging threats.
Limit	Contain	ANNEX I (2)(j)	Requirements to limit attack surfaces and external interfaces enhance the containment of potential incidents.
	Curtail	None	No specific articles focus on curtailing adversarial activities during incidents.
	Recover	None	Recovery mechanisms are not explicitly outlined, indicating a gap in post-incident resilience.
	Expunge	None	No explicit provisions are made for eliminating adversarial traces, such as malware, post-incident.
Expose	Analyze	Articles 14, 15, 16, 50	These provisions emphasize analyzing vulnerabilities and incidents, with mechanisms for coordinated vulnerability disclosures and secure updates.
	Publicize	Articles 17, ANNEX I Part II (6)(7)(8)	Public awareness of vulnerabilities and incidents is supported to enhance collective cybersecurity resilience.

Appendix D

Tactical Objectives and Regulatory Measures Under the Cybersecurity Act (CSA).

TABLE VI
A. Tactical Objectives and Regulatory Measures Under the CSA.

Tactic	Subcategory	Articles	Explanation
Redirect	Deter	Articles 8, 46, 52, 56	These articles establish cybersecurity certification schemes, standardization, and assurance levels to enhance the security of ICT products and services, deterring adversaries by increasing the difficulty of executing successful attacks.
	Divert	None	The Act does not address tactics to divert adversaries to less critical targets, representing a potential area for future regulatory enhancement.

Tactic	Subcategory	Articles	Explanation
	Deceive	None	Deceptive strategies, such as honeynets or false information, are absent, leaving this as a notable gap in the framework.
Obviate	Prevent	Articles 10, 51, 58	These provisions focus on public awareness, secure-by-design principles, and national authority oversight to proactively prevent incidents by ensuring compliance with cybersecurity standards.
	Preempt	None	Preemptive actions, such as disabling adversarial resources before exploitation, are not explicitly addressed in the Act.
Impede	Degrade	None	While measures like multifactor authentication and patch management align with this tactic, they are not explicitly framed within the regulatory language as tools to degrade adversarial progress.
	Delay	None	The regulation does not explicitly promote delaying adversarial actions, such as implementing mechanisms that increase response time or detection opportunities.
Detect	N/A	Article 6(1)(c)	ENISA's role in improving prevention, detection, and analysis capabilities for Union institutions and Member States ensures timely threat identification and situational awareness.
Limit	Contain	None	Containment strategies, such as limiting attack surfaces or interfaces, are not explicitly addressed, representing an area for improvement.
	Curtail	None	Curtailing adversarial activities during incidents is not explicitly covered in the regulatory framework.
	Recover	Article 6(1)(a)	ENISA assists Member States in enhancing their response capabilities, ensuring improved recovery after cyber incidents.
	Expunge	None	Provisions for eliminating adversarial traces, such as malware or compromised data, are not addressed within the Act.
Expose	Analyze	Articles 7(4)(c)(d), 9, 11	Provisions include mechanisms for analyzing vulnerabilities, sharing data, and conducting collaborative threat research to foster continuous improvement in cybersecurity practices.
	Publicize	Articles 7(4)(c)(d), 9, 11	Emphasis is placed on public awareness and responsible disclosure, ensuring information sharing and collaboration to enhance collective cybersecurity resilience.

Appendix E

Tactical Objectives and Regulatory Measures Under the Critical Infrastructure Directive (CID).

TABLE VII
A. Tactical Objectives and Regulatory Measures Under the CID.

Tactic	Subcategory	Articles	Explanation
Redirect	Deter	Article 14	Article 14 mandates background checks for individuals with access to critical infrastructure or sensitive roles, introducing legal and procedural hurdles to discourage adversaries.
	Divert	None	No provisions explicitly address diverting adversaries to less critical targets, such as honeynets or controlled environments.
	Deceive	None	Deceptive tactics, such as deploying false credentials or isolated malware environments, are not addressed by the directive.
Obviate	Prevent	Articles 5, 10, 13(1)(a)(b)(e)(f)	These articles emphasize risk assessments, resilience-building, security requirements, and employee management measures to proactively reduce vulnerabilities. Article 5 focuses on national risk assessments, while Article 13 includes technical, security, and organizational measures.
	Preempt	None	No explicit measures are included to block adversarial access to resources or capabilities before an attack, such as disabling compromised accounts.
Impede	Degrade	None	The directive lacks specific measures to reduce the effectiveness of adversarial actions, such as implementing patching or encrypted data protection.
	Delay	None	There are no explicit tactics to increase the time adversaries require to succeed, such as delaying access to critical systems.
Detect	N/A	Article 15	Mandates timely notification of incidents, including cross-border notifications, ensuring critical entities share information for effective threat detection.
Limit	Contain	None	No specific provisions address containment strategies like isolating infected systems to limit adversarial impact.
	Curtail	None	The directive does not explicitly include measures to curtail adversarial activities or their duration during an incident.
	Recover	Article 13(1)(c)(d)	Article 13 outlines resilience measures, including crisis management protocols, business continuity plans, and alternative supply chains to recover essential services post-incident.

Tactic	Subcategory	Articles	Explanation
	Expunge	Article 13(1)(c)(d)	Article 13 includes protocols for responding to and mitigating incidents, which may involve expunging malicious artifacts.
Expose	Analyze	Article 19	Article 19 establishes the Critical Entities Resilience Group to analyze resilience strategies, share best practices, and facilitate cross-border cooperation among Member States.
	Publicize	Article 19	Article 19 establishes the Critical Entities Resilience Group to analyze resilience strategies, share best practices, and facilitate cross-border cooperation among Member States.

Appendix F

Tactical Objectives and Regulatory Measures Under the Cyber Solidarity Act (CSoA).

TABLE VIII
A. Tactical Objectives and Regulatory Measures Under the CSoA.

Tactic	Subcategory	Articles	Explanation
Redirect	Deter	Article 12	Establishes the EU Cybersecurity Reserve to assist Member States and Union institutions in responding to large-scale incidents, indirectly deterring adversaries.
	Divert	None	No provisions address redirecting adversaries to less critical targets (e.g., honeynets).
	Deceive	None	The regulation does not include provisions to mislead attackers (e.g., misinformation or isolated malware environments).
Obviate	Prevent	Articles 3(2)(c), 8, 10(1)(a), 11	Establishes the European Cyber Shield, emphasizes data and physical security, and supports coordinated preparedness testing across critical sectors.
	Preempt	None	No provisions explicitly address neutralizing adversarial capabilities before deployment.
Impede	Degrade	None	The regulation does not include measures to reduce the effectiveness of adversarial actions (e.g., dynamic patching).
	Delay	None	No explicit measures to slow adversarial progress, such as stricter authentication or dynamic resource allocation.
Detect	N/A	Articles 3(2)(d), 4(1)	Establishes the European Cyber Shield and National SOCs to enhance detection capabilities and improve situational awareness.
Limit	Contain	None	No provisions explicitly address isolating infected systems or restricting adversarial activities.

Tactic	Subcategory	Articles	Explanation
	Curtail	None	The regulation lacks measures to limit the duration or scope of adversarial actions during incidents.
	Recover	Articles 9, 10(1)(b), 13	Establishes the Cyber Emergency Mechanism and EU Cybersecurity Reserve to support response and recovery efforts during large-scale cybersecurity incidents.
	Expunge	Article 9	The Cyber Emergency Mechanism includes actions to remove malicious artifacts and mitigate the impact of incidents.
Expose	Analyze	Article 14	Highlights the EU Cybersecurity Reserve's role in analyzing threats and providing post-incident evaluations.
	Publicize	Articles 3(2)(a)(b), 6, 7	Establishes mechanisms for pooling and sharing data, fostering collaboration, and raising public awareness of cybersecurity threats and vulnerabilities.