Moving Target Defense (MTD) as a Proactive Defense Element for Beyond 5G

Wissem Soussi, Maria Christopoulou, *Member, IEEE,* George Xilouris, Gürkan Gür, *Senior Member, IEEE*

***Abstract*—6G networks will take the digital services offered by 5G to a whole new level with considerably higher bit-rates, lower latency, and ultra reliability. However, the security of these systems is crucial to fulfill the promise of 6G. A critical element of this requirement is the efficient and pervasive security for the protection of 6G infrastructure and services. In this paper, we propose Moving Target Defense (MTD) as a key proactive defense element and elaborate on how it can be integrated into Beyond 5G systems. We also present the relevant research challenges and future research directions including the standardization perspective.**

***Index Terms*—Moving Target Defense (MTD), 6G security, Beyond 5G networks, network softwarization, security management.**

I. Introduction

5G networks are designed to provide a plethora of services as a pervasive enabler for connected and digital applications in anytime-anywhere settings. They are conceptualized as multi-tenant and multi-domain networks with virtualized service/resources running over a flexible software-defined network. These services, ranging from leisure human activities like video streaming to mission-critical applications like smart grids or industrial IoT, should operate in a scalable, cost-efficient, and elastic manner. Beyond 5G or 6G systems will offer a quantum leap over this promise and realize a revolutionary set of services with unprecedented quality and reliability levels such as Further-enhanced Mobile Broadband (FeMMB), Enhanced Ultra-Reliable Low-Latency Communication (ERLLC/eURLLC), and ultra-massive Machine Type Communication (umMTC). They are envisaged to support 1Tbps peak data rate, 1Tbps/m^2 area traffic capacity, and ms level latency. Expected to be deployed in the 2030s, they will unlock advanced traffic demands for more flexible, data-hungry, and tactile applications [1].

However, the increased complexity of this 6G ecosystem will result in a greater attack surface for attackers to exploit, already a pressing issue even with current ongoing 5G developments. In that regard, a malicious agent can perform various attacks such as DDoS, spoofing, or Man-in-The-Middle (MitM), and can even attack from within the network as a single compromised machine/device can lead to widespread security incidents as seen in recent IoT botnets [2]. A great challenge is then to prevent and mitigate attacks toward large-scale 5G and prospective Beyond 5G infrastructure efficiently. It becomes imperative to have an automated system that monitors, proactively protects, detects, and adaptively mitigates the threats by changing the attack surface, performing optimal and dynamic decisions, and considering a multitude of factors in the network operation.

Moving Target Defense (MTD) is a promising protection paradigm that can be used to address these vital challenges. The principle of this conception is to constantly change the configuration and topology of the network and services, making it a dynamic environment [3]. This drastically reduces the action space of malicious users in the *time* and *space* dimensions, as the intelligence gathered with reconnaissance and fingerprinting attacks becomes outdated, inapplicable to network segments, and no more useful for attack strategies. Ideally, MTD will proactively remove the asymmetrical advantage that attackers normally have over network security management — the latter does not know beforehand who the attacker is or what his capabilities are, unlike the former which usually tailors/hones his attack strategies and prepares his attack tools specifically for his target. Nevertheless, the adoption of MTD as a defense element poses an optimization and control problem for security management. To this end, advanced AI/ML techniques are crucial to optimize the MTD strategies for prevention (proactive schemes) and mitigation (reactive schemes), facilitating an autonomous protection approach and guaranteeing the availability of the secured services.

Considering the surging security challenges and need for proactive and autonomous security schemes, MTD integrated with AI/ML is particularly required for Beyond 5G networks. In this paper, we first introduce MTD as an essential defense element for future networks, followed by a discussion on how that integration can be carried out. Then we elaborate on the standardization perspective to identify ongoing activities and potential future efforts with a concrete example based on ETSI NFV SEC specifications. Finally, we present the key research challenges and research directions towards the goal of MTD-integrated 6G networks. Overall, the contributions of our work are as follows:

- We investigate AI/ML powered MTD solutions for Beyond 5G networks from the perspective of cognitive[1] and

Wissem Soussi and Gürkan Gür are with the Zurich University of Applied Sciences (ZHAW), Switzerland. e-mail: {sous, gueu}@zhaw.ch

George Xilouris is with the NCSR Demokritos, Greece. e-mail: xilouris@iit.demokritos.gr

Maria Christopoulou is with the NCSR Demokritos and the University of Peloponnese, Greece. e-mail: maria.christopoulou@iit.demokritos.gr

The research leading to these results partly received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 871808 (5G PPP project INSPIRE-5Gplus). The paper reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains.

[1]Cognitive $\equiv$ concerned with the act or process of observing, learning, knowing, perceiving, and acting (so the system behaves as an environment-aware, learning, and self-acting smart entity)

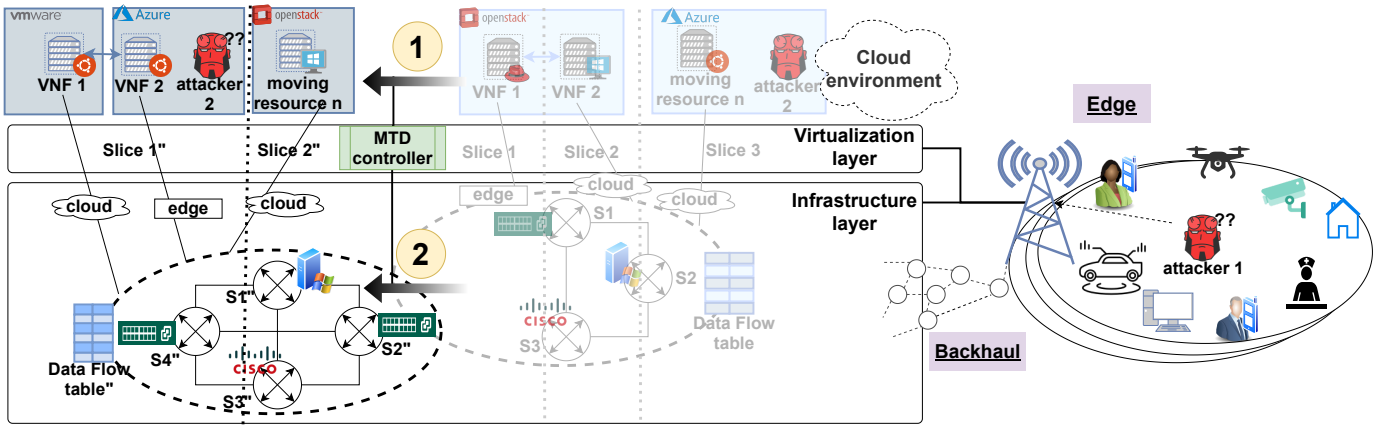

Fig. 1: MTD strategies.

automated security to govern the complex 6G systems;

- We demonstrate the variety of MTD actions that can be performed at different abstraction layers of the NFV environment, characterizing Beyond 5G networks;
- MTD is not considered in the current standardization of security measures for virtualized and software defined networks. We present the standardization aspect by consolidating relevant efforts and potential impact of MTD;
- We identify and present key challenges and research directions for implementing MTD in 6G networks.

II. Technical Background

MTD proactively changes the properties and configurations of an ICT environment, complementing classic security approaches, such as firewalls, security protocols, authentication, and encryption, further increasing the hardening of a networked system. MTD actions are classified into three categories [3]: ***Shuffle***, changing the network (e.g., its topology to make eavesdropping on specific traffic difficult) by moving hosts, proxies, switches, links, and data flow tables; ***Diversity***, changing the technology stack and execution environment, like operating systems, switches with different vendors, protocols, or cloud environment underlying virtual components; ***Redundancy***, creating hardware and software copies, like load balancers, to improve fault-tolerance and reduce risks.

For instance, Figure 1 is a visualization of MTD strategies and how they can be realized in a virtualized and software-defined network. Marker ① shows the MTD *shuffle* and *diversity* schemes that can be performed in a cloud environment to move virtual resources like VNFs and network slice components from a Network Function Virtualization Infrastructure (NFVI) to another (e.g. from VMware to Openstack, or Azure), or change the distribution of a network slice set of resources to different cloud NFVIs, rather than grouping them in a single cloud infrastructure. Marker ② describes the mutation of the infrastructure layer linking different network elements, allowing to change the topology of the network and the traffic of packets with the data flow tables of SDN controllers. Diversity can be added by using different switch vendors (e.g. shuffling OpenVSwitch, Cisco, and Windows switches) or move components from a local cloud at the edge of the network to a remote cloud via Internet.

Previous research has proposed various approaches using shuffle, diversity, and redundancy operations [4], such as network and memory address space randomization, instruction set randomization, and software diversification. They essentially increase the difficulty and time required to discover a target system's configuration by expanding the exploration surface or proactively moving the attack surface. Chai et al. presented DQ-MOTAG [5], a novel MTD framework reusing MOTAG mechanism against DDoS attacks [6] and optimizing it with Deep Reinforcement Learning (DRL). Aydeger et al. [7] explored the usage of an MTD framework in the NFV architecture, preventing Crossfire DDoS attacks and redirecting traffic to virtual shadow networks for deception. Sengupta et al. [8] used the attack graph of a cloud network to formulate a general-sum Markov Game and to solve the Stackelberg equilibrium problem, shown to provide an optimal strategy for the placement of security resources to protect cloud systems.

A. Cognitive techniques for cybersecurity in networks and networked services

Usage of ML/AI and especially deep learning techniques with their performance gains for cybersecurity has recently gained widespread attention [9]. As a promising technique gaining traction in 5G and Beyond 5G security, Deep Reinforcement Learning (DRL) uses deep neural networks (DNN) to accelerate the exploration and learning phase of classic reinforcement learning, which defines agents that receive a reward/penalty based on an environment modeled using Markov Decision Process (MDP) [10]. Here, the agent aims to define an optimal policy that allows him to maximize the return on the rewards. Nguyen et al. [9] surveyed current works on applications of DRL for cybersecurity. As a recent example, Cam presents a method and system for providing cyber resilience by integrating autonomous adversary and defender agents and deep reinforcement learning for predicting the current and future adversary activities, and then by enabling agents to take appropriate automated actions for preventing and mitigating adversary activities in [11].

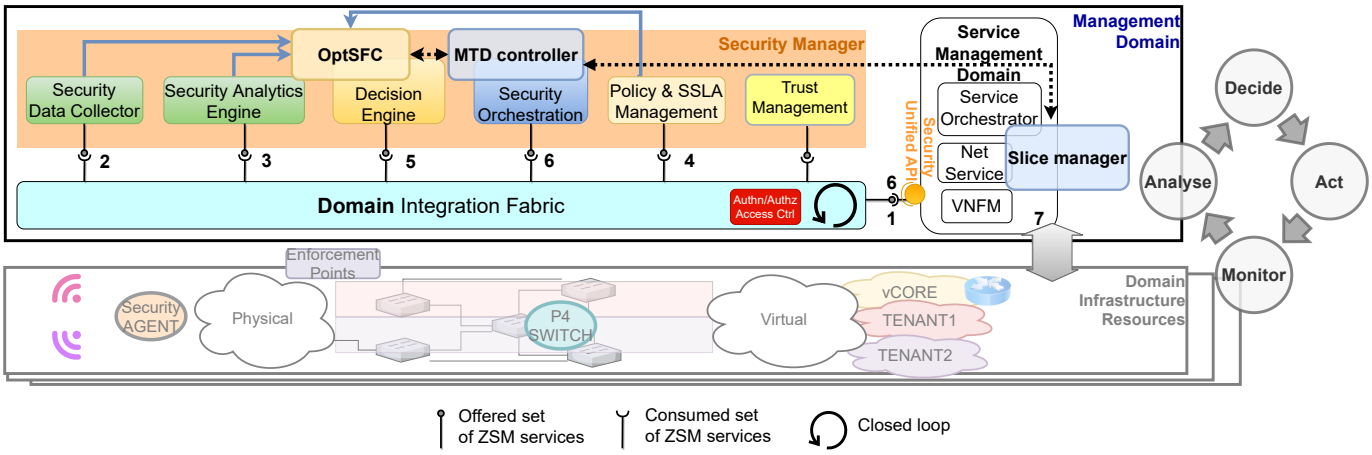

Fig. 2: A closed-loop and pervasive security architecture including MTD and cognitive functions.

Similarly, Taha et al. [12] developed a multi-agent reinforcement framework to solve a two-player general-sum game formulated between an adversary and the defender. Sengupta et al. [13] proposed a multi-agent RL algorithm that uses a Bayesian Strong Stackelberg Q-learning (BSS-Q) approach, improving the MTD for web-application security. To model uncertainty of an MTD system over attacker types and nuances, they used a unifying game-theoretic model, named the Bayesian Stackelberg Markov Games (BSMGs). However, this is not a trivial implementation, as noted in the challenges in Section V.

III. Integration of MTD in Beyond 5G systems at different levels

In a nutshell, the usage of the MTD paradigm would result in an additional security layer for the future networks, in particular Beyond 5G systems. In this section, we present a holistic security architecture for Beyond 5G systems[2] and integrate MTD with AI/ML closed-loop security approach as a proactive security element. To have a concrete security objective, we consider the protection of network slices serving different verticals and use-cases, a situation which will be much more challenging in 6G networks due to QoS and security requirements discussed in Section I. Indeed, to allow the automation of smart closed-loop orchestrations in real-time, this High-Level Architecture (HLA) uses ETSI Zero touch network and Service Management[3] (ZSM)'s definition of a *Management Domain* and a *Domain Integration fabric* to connect the different components of the security management architecture and to enforce the closed-loop work flow of monitoring, analyzing, deciding and acting for all the components [14].

The approach for performing MTD dynamic reconfigurations is to use two different components, one for analytics and cognitive decision making, named ***Optimizer for Security Functions (OptSFC)***, and one for the execution of the MTD action, named ***MTD Controller***. The operational flow of actions of this security mechanism comprises seven subsequent steps: **1**-) The *Service Management Domain* collects data from different data points at the *Domain Infrastructure Resources* level and relay them to the *Security Data Collector*; **2**-) The *Security Data Collector* parses and processes the raw data, feeding them to the *Security Analytics Engine*; **3**-) Different anomaly and attack detection services in the *Security Analytics Engine* generate higher level data, or meta-data, and feed them to the *Decision engine*; **4**-) The *Policy and SSLA (Security Service Level Agreement) management* sets the framework for the MTD actions by feeding the requirements and policy of the related services and verticals; **5**-) *OptSFC* will use ML/AI and modeling techniques such as reinforcement learning and game theory to define an optimal strategy and decide on the MTD action(s) to perform. It is important to note that for proactive strategies the *OptSFC* is not necessarily triggered by a particular event or security alert; **6**-) The MTD controller will then enforce the decided action or action set, including reconfigurations and/or deployment of the appropriate security functions by the *Security Orchestrator* in the relevant slice(s); **7**-) The *Slice Manager* updates the Network Slice Template, communicating with the VNF orchestrator (VNFO), the Virtual Infrastructure Manager (VIM), responsible for the NFVI, and the WAN Infrastructure Manager (WIM); The *Trust Manager* is responsible for the verification and assurance of trust for the execution environments and network elements that provision the resources for the network slice instantiation.

The modus operandi of this scheme is the closed-loop and self-driven operational flow including the cognitive cycle of {monitor, analyse, decide, act} for MTD functionality.

A. OptSFC and Cognitive Techniques (AI/ML Driven Control)

In this section, we present the design of OptSFC with AI/ML functions enabling the adaptive and closed-loop control of MTD operation. OptSFC can be implemented with a custom-modeled DRL algorithm which will be used continuously to adapt MTD actions to changes of the network. For this

[2]This overall security architecture is being developed as part of H2020 RIA INSPIRE-5Gplus project. For further details, refer to https://www.inspire-5gplus.eu/

[3]ETSI ZSM: https://www.etsi.org/technologies/zero-touch-network-service-management

TABLE I: SDOs technical specifications and relevance to MTD.

SDO and working group	Document	Scope	Relevance to MTD
3GPP SA3	TR 33.866 Study on security aspects of enablers for Network Automation (eNA) for the 5G system (5GS) Phase 2; (Release 17) (Draft, work in progress)	Security aspects when using the Network Data Analytics Function for detecting cyber attacks and anomalous behavior	AI/ML, Network automation
3GPP SA2	TS 23.288; Architecture enhancements for 5G System (5GS) to support network data analytics services	Stage 2 architecture enhancements to support data analytics services in the 5G core	AI/ML
ETSI NFV-SEC	ETSI GS NFV-SEC 024; Security Management Release 4 (Work in progress, to be published in 2021)	NFV security management and monitoring	NFV/SDN
	ETSI GS NFV-SEC 025; End-to-end VNF and NS management specification Release 4 (Work in progress, to be published in 2021)	Security management of Virtual Network Functions (VNF) and Network Services (NS). Threats identification.	NFV/SDN
ETSI ENI	ETSI GS ENI 001 V3.1.1 (2020-12); ENI use cases	Use cases for an Experiential Networked Intelligence system, including network security	AI/ML
ETSI SAI	ETSI GR SAI 001; Threat Ontology (Draft, work in progress, to be released in 2021)	Definition of AI threats	AI/ML
	ETSI GS SAI 002; Data Supply Chain (Draft, work in progress, to be released in 2021)	Identification of methods used to source data. Mechanisms for preserving data integrity and confidentiality.	AI/ML
	ETSI GR SAI 004 v1.1.1 (2020-12); Problem Statement	Securing AI-based systems problem description. Description of real-world use cases and attacks.	AI/ML
ETSI ZSM	ETSI GS ZSM 001 V1.1.1 (2019-10); Requirements based on documented scenarios	Scenarios on E2E network and service management, analytics and machine learning	AI/ML, Network automation
	ETSI GS ZSM 010; General Security Aspects (Draft, to be published in 2021)	Security threat and risk analytics on ZSM framework and attack mechanisms	Network automation
ITU-T FG-ML5G	Y.Sup55 : ITU-T Y.3170-series - Machine learning in future networks including IMT-2020: use cases	Use cases for machine learning in future networks including IMT-2020. They include security use cases, as well.	AI/ML

purpose, the operational environment is formally defined with a game theory model using Markov Decision Process (MDP). In this context, the model can be defining one single agent, the MTD controller, who solely acts based on the change of the network state, focusing on proactive defense and attack prevention. Here, a state of the environment is represented by a set of verticals, network slices, and VNFs, detailed by their description, their importance and their condition (for risk analysis and threat level determination).

An alternative model can include an additional agent, namely the attacker, enabling the MTD controller to further improve its *reactive* defense and attack mitigation. The environment and game theory model present added parameters for the attacker's identification and the prediction of his target [12]. Attackers' strategies can change with time, therefore the model needs to describe high-level attack patterns able to identify old and new attacks by analyzing behaviours and predicting the intentions (e.g., reconnaissance, Denial of Service (DoS), Command and Control (C&C), MitM, etc..). The advantage of this multi-agent model is the possibility for experimenting the implementation of an autonomous unsupervised learning system, conceptually similar to Neural Fictitious SelfPlay (NFPS) [15], simulating Red Team/Blue Team games where the two agents (the MTD controller and the attacker) are autonomously learning "from scratch", without predefined domain knowledge except for the game rules.

IV. Standardization Activities and Future Perspective

From a standardization perspective, MTD has not been the subject of any related activity among Standardization Organizations (SDOs). However, MTD leverages three existing technologies for its implementation: i) AI/ML, ii) NFV/SDN, and iii) Network Automation, which are being worked on in various standardization activities. These three mechanisms will enable MTD in a practical way and their proper operation already presents new challenges and requirements in 5G and Beyond 5G networks. There has been a considerable amount of technical specifications and reports published on these mechanisms. We provide the most representative ones in Table I. The benefit of our discussion in this section is twofold: The first is related to the future networks' perspective – we identify the standardization efforts which will be crucial for Beyond 5G systems. The second is a relatively short-term one: we also highlight how they can be utilized/developed for MTD integration in emerging 5G networks. Accordingly, the specific example in Section IV-A serves both purposes.

3GPP has already addressed the use of AI/ML in the 5G Core Service Based Architecture (SBA), by introducing the Network Data Analytics Function. This function provides analytics and notifications to other network functions regarding the users' behavior and the network's status. 3GPP SA3 is currently working on a draft TR identifying the security issues, requirements, and solutions regarding Network Slicing and the use of the Network Data Analytics Function in selected use cases. This kind of functionality can be expanded and serve for MTD in next iterations targeting Beyond 5G.

As a multi-pronged effort, ETSI has launched multiple Industry Specification Groups (ISG) to examine 5G component technologies, including NFV (ETSI NFV), AI (ETSI ISG Securing Artificial Intelligence-SAI, ETSI ISG Experiential

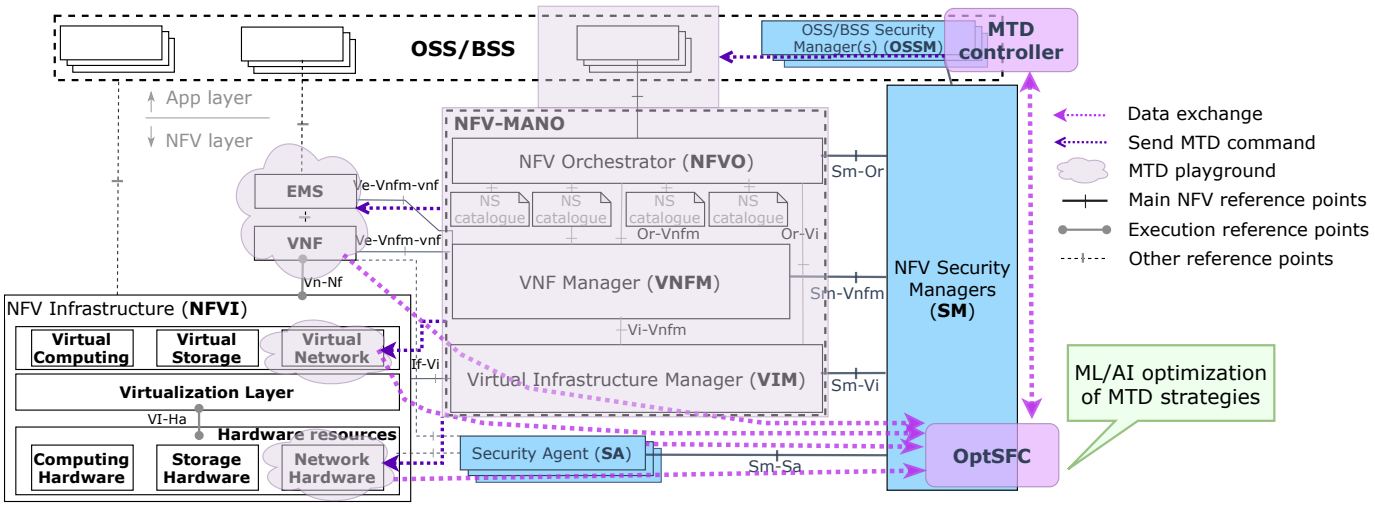

Fig. 3: Integration of MTD security in the ETSI NFV security architecture.[4]

Network Intelligence - ENI) and network automation (ETSI ISG Zero touch and service management - ZSM). NFV-SEC is a WG under ISG NFV that produces industry specifications on security-related matters of NFV technology. Since 2014, the NFV SEC WG has produced multiple Group Specifications (GS) and Group Reports (GR). Work during releases 3 and 4 of ETSI NFV has increased the focus on security specifications as the scope and features of NFV platforms are expanding. These specifications are important as focus points to extend and enable MTD capability for both 5G and Beyond 5G systems.

ETSI ZSM ISG was established in 2017, to define specifications regarding end-to-end network automation of service provisioning and lifecycle management in highly heterogeneous networking environments, such as 5G and future 6G systems. ETSI ZSM is defining the ZSM Framework that allows the self-optimization improvement of the network, according to specified SLAs. The network is separated into discrete management domains, each with its closed-loop operation process, subject to an overarching *End-to-End Service Management Domain*, that is responsible for the overall service provisioning to the customer. ETSI ZSM builds upon AI and network slicing to enable its vision. From a security perspective, ISG ZSM is currently working on a draft specification *GS 010 on General Security Aspects of the ZSM Framework*, providing a comprehensive list of threats stemming from its operation.

ETSI ISG ENI was also launched in 2017 to define a Cognitive Network Management architecture, using AI techniques and context-aware policies to adjust offered services based on changes in user needs, environmental conditions, and business goals. The ISG has produced a set of use cases, including network security, where the ENI system can detect various attacks and trigger a reaction by the network. Another group, ETSI ISG SAI, was formed in 2019 and aims to develop technical specifications to alleviate threats emerging from deploying AI and threats targeting AI systems originating from other AI systems and typical attack sources. This ISG has undertaken the tasks of defining AI threats, provide relevant use cases, recommend mitigation measures against such threats, and provide possible recommendations regarding data sharing. At a global level, ITU has established the ITU-T Focus Group on ML for Future Networks (FG-ML5G) working on technical specifications for machine learning for future networks, including interfaces, network architectures, protocols, algorithms, and data formats.

It is important to reference that many industry fora, like NGMN, 5G Americas, 5G-PPP, GSMA, and agencies like ENISA and FCC, have published technical reports regarding potential threats identified in 5G networks. These threats fall under the entire spectrum of 5G technologies, including NFV, AI, and network slicing, and have implications for Beyond 5G systems. These reports provide a thorough threat landscape, where MTD–as an emerging technology- can be deployed to mitigate different attack scenarios.

A. Integration in the NFV Security Architecture

The ETSI NFV standards define a good candidate architecture to integrate MTD in Beyond 5G networks as well as in 5G systems. This ISG is currently working on improving the security of such architecture, with additional components like the OSS/BSS security managers (OSSM), NFV Security Managers (SM) and security agents (SA). The standardization is in progress, and MTD can be effectively integrated in upcoming iterations for future networks, as depicted in Figure 3.

In such an integration, at the NFVI layer, the MTD controller would modify the virtual network in the cloud environment or the data plane flow at the Network Hardware with the help of the VIM and its SDN controller. At the VNF layer, instead, it can move single VNFs or whole network services from a NFV infrastructure to the other. A network service provider can improve MTD effects by using VIMs that control a diverse set of NFVIs, combining both *shuffle* and *diversity* schemes at the cloud level (as previously shown in Figure 1). Another possibility is to communicate with the WIM to dynamically change the transport network graph, so

[4]ETSI NFV Rel. 4 Security; Security Management Specification: GS NFV-SEC 024 v.0.0.5 Draft

TABLE II: Research Challenges and Directions for MTD in 6G security management.

Research Challenges	**Key research topics**	**Key Points**
Architectural challenges	Full-stack and full-spatiotemporal MTD action space	Exploit different virtualization layers to maximize MTD entropy
	Low-complexity integration	Efficient MTD mechanisms and interface design for network scalability and flexibility
	Evolution of 5G specifications to 6G	New architectural elements, capabilities needed in existing specifications on AI/ML, orchestration and virtualization
6G applications and requirements	FeMMB	Overhead minimization, how to implement distributed MTD solutions for local security
	Extreme massive connectivity (umMTC)	Scalability, impact on OSS/BSS for monitoring and accounting of sharing
	ERLLC/eURLLC	Latency minimization for delay-sensitive applications
AI/ML related challenges	Unsupervised Self-Play RL	Representative Markov modeling, AI explainability, and unsupervised learning evaluation
	Efficient models and optimal action management	What/When/Where/How to move, combination of proactive and reactive schemes and minimalist action enforcement
	Secure AI for cybersecurity	AI ethics and liability, AI unfairness, privacy, trustworthy data support and careful RL modeling
Testing, validation and integration	Test case realization	Realistic and feasible test case design and testbed implementation
	Realistic security KPIs	KPI formulation for 6G use cases
Orchestration and management	Heterogeneous network architectures	Synchronization/federation of different MTD elements in multi-tenant environments
	Fundamental limits	Identification of security management capabilities attainable with MTD
	Reliability	Consistent performance and robustness against different security incidents

the WIM can reserve the 5G WAN resources and enable dynamic transparent E2E connectivity using SDN rules.

As these mutations are performed on different abstraction layers, MTD actions come with different costs. This has to be considered during the optimization strategy and decision making of the OptSFC component, improving the cost/effectiveness ratio of the MTD controller. This is an important research challenge as noted in Section V-C.

V. Challenges and Future Research Directions

This section focuses on research challenges which need to be addressed while integrating MTD as part of a security architecture for 5G and Beyond 5G networks. They are discussed below as well as summarized in Table II.

A. Architectural Challenges

The MTD techniques studied in the literature commonly focus on a singular aspect of the MTD and related security requirements. The integration and use of full-stack, full-spatiotemporal action space (e.g., VM live migration, OS diversification, hybrid diversity, shuffle, and redundancy actions) in virtualized infrastructure (multiple layers of the software stack) for inherent entropy maximization goal of MTD is still scarcely explored.

Learning-based optimization of autonomous and proactive security is architecturally challenging due to the heterogeneity of services, infrastructure, and operational requirements. One major question is how to integrate MTD and AI/ML for protection of various strata in 6G as we formulate that new generation of wireless networks. As presented in Section IV, how the current 5G specifications shall evolve to allow that adoption for 6G is another grand challenge. That last research question includes the definition and design of required new interfaces and new capabilities in the fundamental network elements and in the security management framework that will emerge with 6G.

B. Challenges due to 6G Applications and Requirements

The envisaged 6G applications and thus requirements will pose formidable QoS and service level challenges. In that regard, *FeMBB* expects extreme high data rates to serve 6G verticals. However, such Tbps bitrates are incredibly challenging for traffic processing in security functions in the network. This complexity issue will challenge MTD solutions as well since they will incur additional overhead in terms of monitoring, event processing, and countermeasure enforcement. Therefore, how to design and implement distributed MTD solutions is an important research topic since traffic should be processed locally and on-the-fly at different points in the network.

With the emergence of Internet of Everything (IoE), *umMTC* involves extreme massive connectivity use cases including critical ones that impose much more stringent security requirements compared to current 5G counterparts. In that regard, devices and software elements with remarkably diverse capabilities will challenge the deployment of security solutions. Although the hardware capabilities will further develop, there will still be resource-constrained devices, especially with the emergence of extremely demanding applications. As a mobile network, 6G will also meet much higher mobility compromising the protection impact of security enforcement because of attachment changes in the edge. Like umMTC, the high reliability and low latency requirements in *ERLLC/eURLLC* make the latency impact of MTD security workflows an important research question. High reliability also calls for

highly effective security solutions protecting the availability of services at an extreme level. This requirement also has a design impact on MTD solutions such as DDoS-oriented protection goals.

C. AI/ML Related Challenges

To date, there is no blueprint for designing and operating learning-based optimized MTD for large-scale network scenarios. While RL-driven MTD promises self-regulated autonomous operation and mitigation of cyber threats, its fundamental advantages and impact have not been identified in various security scenarios. When dealing with RL, complex models using Multi-agent DRL further increases the system requirements, as more high-quality data is needed from the security agents and monitoring systems for the learning algorithms. Unsupervised RL with Self-Play simulations needs careful modeling to avoid unrealistic experiences from which agents learn inappropriate strategies that are inapplicable in the real system. For this problem, an additional notion of AI explainability is needed to better evaluate unsupervised models.

Another major challenge is the improvement of MTD efficiency, achievable by reducing the MTD overhead to its minimum, performing only necessary and useful mutations, based on the network state, and real-time risk and threat analysis. To measure such efficiency is also a challenge, as it is determined with a specific MTD action cost and its effectiveness against a specific attack, especially for all the combinations of MTD actions and attacks. The cohabitation of proactive (i.e., to change attack surface before the attack) and reactive actions (i.e., to change attack surface and minimize the impact during the attack) supported by online network monitoring for situational awareness is still to be investigated for 6G networks. Many other classic problems related to AI/ML are being addressed by SDOs and working groups, like AI ethics, who is liable if the AI fails, how to avoid AI inducted unfairness (not to starve some users or applications), prevention of sensitive data leak (e.g., when ML functions are distributed over the network), and robustness to "poisonous" data injection (for instance, done to trigger unnecessary MTD actions, slowing down the system and resulting in a DoS attack).

D. Testing, Validation and Integration Challenges

Most of the proposed cognitive MTD solutions for current and emerging networks are evaluated on relatively simplistic scenarios and limited environments, i.e., based on a static instantiation of a system model, which is used to develop cognitive security schemes and optimization mechanisms. However, more realistic environments are highly dynamic and heterogeneous, resulting in fast variations of the virtual service and network topology over time. The main problem for Beyond 5G or 6G is faithful and realistic testing and validation for pre-standardization work since these systems are not standardized yet and in early-stage discussions. Additionally, security KPIs for 6G are yet to be investigated and determined. Therefore, how to use available 5G platforms, modified considering 6G use-cases and applications with testing and validation goals tuned for 6G, is an important research question. Dealing with the formidable dynamics stemming from 6G vision in more realistic security scenarios is an essential challenge.

E. Orchestration and Management Challenges

The correlation of MTD with network slicing in 5G and Beyond deployments, is challenging for the Management and Orchestration systems. The factors that affect the capability of the frameworks to cope with the imposed requirements are mainly velocity, isolation, slice topology complexity, trust, and locality. The first factor is related to the capability of the orchestration framework to change either pro-actively or re-actively the slice topology maintaining the service graph while maintaining the service operation. The second factor is isolation, i.e. preserving the isolation and trust between the slice topology changes. The network slice topology complexity increases the signaling overhead affecting the timely transition between the topology instances. MTD acts upon a provisioned and instantiated network slice and modifies the provisioned resource locations altering network path and execution environments, as such trust management poses a challenge that may affect the time required for transcending from one configuration to another. Lastly, the locality of the migrations and mutations that have to occur for each transition also imposes challenges. For example, the mutation of slice topology within a cloud infrastructure, e.g. migration from one node to another, is less demanding than migrating to another cloud infrastructure.

VI. Conclusion

In this paper, we present and discuss MTD as a key proactive defense element to realize efficient and pervasive security for protecting Beyond 5G infrastructure and services. We also present the relevant research challenges and future research directions including the standardization perspective.

References

[1] I. F. Akyildiz, A. Kak, and S. Nie, "6G and beyond: The future of wireless communications systems," *IEEE Access*, vol. 8, pp. 133 995–134 030, 2020.

[2] A. Marzano, D. Alexander, O. Fonseca, E. Fazzion, C. Hoepers, K. Steding-Jessen, M. H. P. C. Chaves, I. Cunha, D. Guedes, and W. Meira, "The evolution of bashlite and Mirai IoT botnets," in *2018 IEEE Symposium on Computers and Communications (ISCC)*, 2018, pp. 00 813–00 818.

[3] J. H. Cho, D. P. Sharma, H. Alavizadeh, S. Yoon, N. Ben-Asher, T. J. Moore, D. S. Kim, H. Lim, and F. F. Nelson, "Toward proactive, adaptive defense: A survey on moving target defense," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 709–745, Sep. 2020.

[4] A. Chowdhary, A. Alshamrani, D. Huang, and H. Liang, "MTD analysis and evaluation framework in software defined network (mason)," in *Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization*, ser. SDN-NFV Sec'18. New York, NY, USA: Association for Computing Machinery, 2018, p. 43–48.

[5] X. Chai, Y. Wang, C. Yan, Y. Zhao, W. Chen, and X. Wang, "DQ-MOTAG: Deep reinforcement learning-based moving target defense against DDoS attacks," in *2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC)*. IEEE, Aug 2020, pp. 375–379.

[6] Q. Jia, K. Sun, and A. Stavrou, "MOTAG: Moving target defense against internet denial of service attacks," in *2013 22nd International Conference on Computer Communication and Networks (ICCCN)*, 2013, pp. 1–9.

[7] A. Aydeger, N. Saputro, and K. Akkaya, "A moving target defense and network forensics framework for ISP networks using SDN and NFV," *Future Generation Computer Systems*, vol. 94, pp. 496–509, may 2019.
[8] S. Sengupta, A. Chowdhary, D. Huang, and S. Kambhampati, "General sum markov games for strategic detection of advanced persistent threats using moving target defense in cloud networks," in *Decision and Game Theory for Security*, T. Alpcan, Y. Vorobeychik, J. S. Baras, and G. Dán, Eds. Cham: Springer International Publishing, 2019, pp. 492–512.
[9] T. T. Nguyen and V. J. Reddi, "Deep reinforcement learning for cyber security," 2019. [Online]. Available: https://arxiv.org/abs/1906.05799
[10] D. P. Bertsekas, *Reinforcement Learning and Optimal Control*. Athena Scientific, 2019.
[11] H. Cam, "Cyber resilience using autonomous agents and reinforcement learning," in *Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications II*, T. Pham, L. Solomon, and K. Rainey, Eds., vol. 11413, International Society for Optics and Photonics. SPIE, 2020, pp. 219 – 234.
[12] T. Eghtesad, Y. Vorobeychik, and A. Laszka, "Adversarial deep reinforcement learning based adaptive moving target defense," in *Decision and Game Theory for Security*, Q. Zhu, J. S. Baras, R. Poovendran, and J. Chen, Eds. Cham: Springer International Publishing, 2020, pp. 58–79.
[13] S. Sengupta and S. Kambhampati, "Multi-agent reinforcement learning in Bayesian Stackelberg Markov games for adaptive moving target defense," 2020. [Online]. Available: https://arxiv.org/abs/2007.10457
[14] J. Ortiz, R. Sanchez-Iborra, J. B. Bernabe, A. Skarmeta, C. Benzaid, T. Taleb, P. Alemany, R. Muñoz, R. Vilalta, C. Gaber, J.-P. Wary, D. Ayed, P. Bisson, M. Christopoulou, G. Xilouris, E. M. de Oca, G. Gür, G. Santinelli, V. Lefebvre, A. Pastor, and D. Lopez, "INSPIRE-5Gplus: Intelligent security and pervasive trust for 5G and beyond networks," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ser. ARES '20. New York, NY, USA: Association for Computing Machinery, 2020.
[15] J. Heinrich and D. Silver, "Deep reinforcement learning from self-play in imperfect-information games," mar 2016. [Online]. Available: http://arxiv.org/abs/1603.01121

Wissem Soussi is a research assistant at Zurich University of Applied Sciences (ZHAW).He undergraduated in 2018 on Computer Sciences from Montpellier University, and obtained the Msc. degree on Cybersecurity in 2020 from Grenoble University, France. His topics of interest are networks & systems security and ML/AI applied to cybersecurity.

Maria Christopoulou is a Research Associate at the Institute of Informatics and Telecommunications in NCSR "Demokritos". She is currently a Ph.D candidate at the University of Peloponnese (UoP) in the field of resource management in cellular telecommunication systems. She holds a BSc in Physics (2014) and a MSc in Radioelectrology and Electronics (2016) from the National and Kapodistrian University of Athens.

George Xilouris received his B.Sc. degree in Physics in 1999 from University of Ioannina and his M.Sc. degree in Automation Systems from National Technical University of Athens (NTUA) in 2000. Since 2000 he is working as Research Fellow at the Institute of Informatics and Telecommunications in NCSR "Demokritos". His research interests include Software Networks, Network Management and future network architectures, 5G communications and performance evaluation.

Gürkan Gür is a senior lecturer at Zurich University of Applied Sciences (ZHAW), Switzerland. He received his B.S. degree in electrical engineering in 2001 and Ph.D. degree in computer engineering in 2013 from Bogazici University. His research interests include Future Internet, information security, next-generation wireless networks and ICN.