DDoS Defense using MTD and SDN

Jessica Steinberger*†, Benjamin Kuhnert*, Christian Dietz‡†, Lisa Ball*,
Anna Sperotto†, Harald Baier*, Aiko Pras† and Gabi Dreo‡

*da/sec - Biometrics and Internet Security Research Group
University of Applied Sciences Darmstadt
Darmstadt, Germany
Email:{Jessica.Steinberger, Benjamin.Kuhnert,
Lisa.Ball, Harald.Baier}@h-da.de

‡ Research Institute CODE
Universität der Bundeswehr München,
Neubiberg, Germany
Email:{Christian.Dietz,
Gabi.Dreo}@unibw.de

†Design and Analysis of Communication Systems
University of Twente
Enschede, The Netherlands
Email:{J.Steinberger, A.Sperotto,
A.Pras}@utwente.nl

***Abstract*—Distributed large-scale cyber attacks targeting the availability of computing and network resources still remains a serious threat. In order to limit the effects caused by those attacks and to provide a proactive defense, mitigation should move to the networks of Internet Service Providers. In this context, MTD is a technique that increases uncertainty due to an ever-changing attack surface. In combination with SDN, MTD has the potential to reduce the effects of a large-scale cyber attack.**

In this paper, we combine the defense techniques moving-target using Software Defined Networking and investigate their effectiveness. We review current moving-target defense strategies and their applicability in context of large-scale cyber attacks and the networks of Internet Service Providers. Further, we enforce the implementation of moving target defense strategies using Software Defined Networks in a collaborative environment. In particular, we focus on ISPs that cooperate among trusted partners. We found that the effects of a large-scale cyber attack can be significantly reduced using the moving-target defense and Software Defined Networking. Moreover, we show that Software Defined Networking is an appropriate approach to enforce implementation of the moving target defense and thus mitigate the effects caused by large-scale cyber attacks.

I. Introduction

Large-scale cyber attacks still remain the top cause for network and service outages in recent years [1], [2]. The reason is that these attacks are getting more frequent, more sophisticated and increasingly impacting network operators of high-speed networks [3], [4]. At the same time, the launch of large-scale cyber attacks is getting easier through offerings of DDoS-as-a-Service websites [5], hire-a-botnet-services [6] and is encouraged by the static configuration of cyber systems [7]. This static configuration supports attackers (a) to perform a reconnaissance of the target system, study and determine its potential vulnerabilities and (b) choose the best setup to perform a devastating large-scale cyber attack [8]. Moreover, traditional mitigation solutions (e.g., firewalls, Intrusion Prevention Systems) are often not able to handle the large amount of traffic reaching the target network [3] and the use of cloud-based or content-delivery-based mitigation solutions often cause high economic costs [9].

One approach to handle large-scale cyber attacks is to collaborate among trusted partners. However, collaborative approaches have predominantly focused on attack detection in the last years, but solutions for collaborative mitigation and response measures in high-speed networks are missing [10]. At the same time, approaches using Software Defined Networking (SDN) and Moving Target Defense (MTD) have been published and are currently attracting increasing interest from research and industry. However, the use of MTD is still in its initial phase [7], [11] and to the best of our knowledge only one publication focuses on a collaborative use of SDN in context of high-speed networks [12].

To overcome the lack of an effective, collaborative and scalable mitigation approach, this paper presents a Distributed Denial of Service (DDoS) defense solution using MTD and SDN in context of high-speed networks. The advantage of a collaborative DDoS defense solution is that each participating partner achieves insights into the current threat landscape that would otherwise not be obvious. Further, collaborative DDoS defense pools expertise and resources of all collaborating partners and does not propagate malicious traffic further through the network. We enhance our collaborative DDoS defense solution by means of MTD. The advantage of MTD is that it limits the attackers knowledge of the attack target due to its ever-changing attack surface and thus increases the difficulty to launch a successful attack. Our approach of MTD is implemented using SDN. The contribution that our work brings to the state of the art is that (i) it combines the use of MTD and SDN to limit the effects caused by large-scale cyber attacks in context of high-speed networks. Further, our collaborative DDoS defense solution (ii) provides a low cost solution that easily integrated into existing infrastructure [13]. (iii) In the evaluation of our approach, we also extend the theoretical model for determining the effectiveness of MTD systems in enterprise networks presented in Zhuang et al. [14], which we use to determine the effectiveness of our collaborative DDoS defense solution.

The remainder of this paper is structured as follows. Section II introduces the terminology used throughout this paper. In Section III we describe a scenario in which the defense strategies MTD is used and define requirements to make use of MTD and SDN within high-speed networks. Published related work in the area of MTD, SDN and mitigation of large-scale cyber attacks is presented in Section IV. Section V introduces our DDoS defense solution. In Section VI we evaluate current MTD strategies using SDN regarding their strength

and weaknesses especially in terms of their applicability in context of Internet Service Provider (ISP) networks and their effectiveness to mitigate large-scale cyber attacks. Finally, the results are discussed and concluded in Section VII.

II. Terminology

In this section, we introduce terms related to MTD and SDN that are used throughout the paper and thus support better understandability of our work. In Section II-A, we introduce MTD, review current MTD strategies and their applicability in context of large-scale cyber attacks and the networks of Internet Service Providers. Next, we introduce SDN and investigate its use to enforce the implementation of MTD strategies in a collaborative, high-speed environment in Section II-B.

A. Moving-Target Defense

Moving Target Defense (MTD) is the concept of controlling changes across multiple system dimensions in order to increase uncertainty and apparent complexity for attackers, reduce their window of opportunity and increase the costs of their probing and attack efforts [15], [16]. In the area of MTD, we adhere to the terminology defined and used in [7] and [8]:

A MTD system, Σ, is a tuple of (Γ, G, P) where Γ is a configurable system, G is a set of operational and security goals, and P represents a set of policies. A configuration system Γ is a tuple of (S, Λ, τ) where $S = \{s_1, s_2, \ldots, s_n\}$ is a set of configuration states the MTD systems can be in, $\Lambda = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ a set of actions, and $\tau : S \times \Lambda \rightarrow S$ is the state transition function. A configuration state, s, is a unique assignment of value(s) z from a configuration parameter type Π to a configuration parameter π. A configuration parameter type Π refers to the domain of possible values that a configuration parameter π can assume. A configuration parameter π can take a value based on its configuration type Π to specify the details of the configuration. An example of a host configuration Π is shown in Equation (1).

$$\overbrace{\underbrace{\text{IP address}}_{\text{configuration parameter } \pi} = \underbrace{192.168.0.54}_{z}}^{\text{configuration state } s \text{ where } s=\pi \leftarrow z} \tag{1}$$

In recent years, several MTD strategies have been published which can be grouped into three main categories: (i) network-level MTD, (ii) host-level MTD and (iii) application-level MTD [17]. The network-level MTD refers to changes of the shape of the network graph (e.g., IP-hopping, random port numbers, extra open or closed ports, fake listing hosts). The host-level MTD focuses on changes at the host and operating system (e.g., naming, configuration). Changes on application types and versioning, randomly arranging memory layout are grouped into the application-level MTD.

B. Software-Defined Networking

Software-defined Networking (SDN) [18] is a network paradigm, which decouples the control and the data plane of a network device. While the data plane still resides on the device, the control plane is outsourced to a centralized controller. The control plane and the data plane communicate over a so called southbound interface. The most common southbound protocol is the OpenFlow protocol [19], which is standardized by the Open Networking Foundation (ONF). The controller also provides a centralized network overview over the northbound API and is responsible for high-level decisions like routing. In contrast to the southbound API, there is no standardization for the northbound interface. The data plane is still responsible for packet-forwarding. Incoming packets are matched against packet header fields.

III. Scenario, Requirements and Assumptions

In this section, we describe the main focus of this work. First, we define the networks in which we are going to place MTD and SDN. Second, we define the requirements that MTD using SDN should fulfill, as they emerged by the scenario described in Section III-A. In the following, we will use these requirements to evaluate MTD using SDN in the context of large-scale cyber attacks and the network of ISPs.

A. Scenario

The focus of this work are high-speed networks using a link speed of multiple 10 Gbps. In addition, we assume the networks in our scenario implement an architecture of a typical flow monitoring setup [20] and provide the capability to use SDN. Besides, the availability of flow data and the technical capability of SDN, we assume that network operators cooperate among trusted partners to minimize or prevent damages caused by large-scale cyber attacks. The exchange of security events is in accordance to the communication process described in Steinberger et al. [10]. The main advantage of a collaborative approach is to move from a reactive to a proactive approach and to gain insight into the current threat landscape that otherwise would not be obvious.

B. Requirements

In this section, we introduce 9 requirements that a DDoS defense using MTD and SDN should fulfill. The requirements are part of the Theory of Moving Target Defense described in [7], the operational requirements presented within the IETF DDoS Open Threat Signaling (DOTS) working group [21] and of the Software Defined Exchange (SDX) introduced in [12]. Our requirements are:

a) Diversification: A DDoS defense solution using MTD within the network of Internet Service Providers should support multiple configuration choices [7] to avoid static configurations of the high-speed networks.

b) Adaptations: A DDoS defense solution using MTD should support movements within the system that do not change the shape of the network graph and also support transformations that changes the size and shape of the network graph [7].

c) Randomization: Configuration randomization provides the possibility to make use of the full available configuration space and thus the DDoS defense solution should have the capability to support configuration randomization and thus ensure unpredictability.

d) MTD Entropy: The effectiveness of a DDoS defense solution using MTD should be measured by using the MTD Entropy presented by [7].

e) Ease of Deployment: A DDoS defense solution and its underlying implementation (e.g., MTD and SDN) should support platform independence. Further, the DDoS defense solution should be able to handle different types of large-scale cyber attacks. The platform independence and the reusability with different types of large-scale cyber attacks ensures that it easily integrates with the existing infrastructure.

f) Timeliness: The adaptations of the DDoS defense solution should be performed in an appropriate amount of time to support a proactive network-based attack detection and mitigation.

g) Scalability: A collaborative DDoS defense using MTD and SDN should support hundreds of collaborating partners. As a result, conventional SDN switches should be able to handle hundreds of thousands of IP prefixes and matching rules while limiting rule-table size and computational overhead [12].

h) Wide-area load balancing: In order to limit the effects and mitigate a large-scale DDoS attack, collaborating partners should bundle resources and perform wide-area load balancing in case of an ongoing large-scale attack. This wide-area load balancing should divide the attack traffic over a bundle of resources, based on packet-handling rules [22] installed using SDX [12].

i) Cost-conscious: ISPs are often geographically expansive and the use of MTD and SDN should either make use of existing hardware or the solution should avoid to be place middleboxes at every location to achieve a cost-conscious DDoS defense solution.

C. Assumptions

The use of MTD strategies have to ensure a consistent and valid network configuration. This topic is currently under active study in literature, with focus on the effect of *Adaptation Selection* and *Timing Problem* on the transition between consistent and valid network configuration states and the creation of invalid network configuation states [7], [23]. We consider however this topic to beyond the scope of this paper, and for the research we conduct we always assume a consistent and valid network configuration state and thus predefine possible valid network configuration states.

IV. Related work

In this section, we present related work that has been published in the area of MTD, SDN and mitigation of large-scale cyber attacks.

In 2009, the Networking and Information Technology Research and Development (NITRD) Program introduced the initial concept of MTD as a new promising approach to cyber security [15]. This concept has been formalized by Zhuang et al. [7] in 2014. The authors presented a theory of MTD systems that defines the key concepts and their basic properties. In 2015, the authors presented a theory of cyber attacks to complement the theory of MTD systems [8].

In [24], [25], the authors introduced MOTAG, a moving-target defense approach against network-based flooding attacks. MOTAG relies on a hidden proxy-based shuffling approach to separate the attackers from benign clients and uses an intermediate layer with a pool of geographic distributed proxies. However, MOTAG requires client authentication and thus it is not suitable to mitigate DDoS attacks targeting network infrastructure and services used by anonymous users. In addition, MOTAG is not able to mitigate different types of large-scale cyber attacks (e.g., application-layer DDoS attacks). In [26], Jia et al. presented a successor of MOTAG, that supports authenticated and anonymous clients and is deployed in a cloud-based environment. Both MTD approaches [24]–[26] were only simulated in MATLAB and are vulnerable to the *proxy harvesting attack* [27].

In [28], Wright et al. presented a game-theoretic analysis of the four used MTD strategies (i) proactive server migration, (ii) use of client count signal by attacker, (iii) blocking suspected insiders, (iv) delayed attack timing) that are likely to be used in large-scale cyber attacks. This game-theoretic analysis is founded on settings in MOTAG and its successor.

MacFarland et al. [29] presented an MTD approach using a host-based SDN to distinguish between trustworthy and untrustworthy clients within a single network. However, the authors do not consider the use of MTD and SDN in a high-speed environment to mitigate large-scale cyber attacks.

An analytical model to analyze the effects of MTD is presented in [14]. However, Zhuang et al. [14] focus on enterprise networks and the propagation of compromises of nodes within this enterprise network.

In the area of SDN-enabled MTD for cloud environments, the work of Debroy et al. [30] and Chowdhary et al. [31] has been published. However, Steinberger et al. [13] revealed that ISPs do not consider to make use of cloud-based mitigation.

In [32], Ager et al. investigated the anatomy of a large European Internet Exchange Point (IXP). They found that the largest IXP carries petabytes of network traffic on a daily basis and are similar to large high-speed networks. Gupta et al. [12] investigated the use of SDN in networks of IXPs and introduced SDX. They described an IXP network as a layer 2 network, consisting of layer two fabrics, in which participating networks exchange Border Gateway Protocol (BGP) routes and direct network traffic to other participants. SDX provides network operators the possibility to control the flow of network traffic entering and leaving border routers. In order to learn BGP routes, Gupta et al. [12] used a SDX controller that integrates a route server. Further more SDX is based on Pyretic and use OpenFlow. However, Gupta et al. [12] did not combine SDX with MTD in order to mitigate the effects of a large-scale cyber attack.

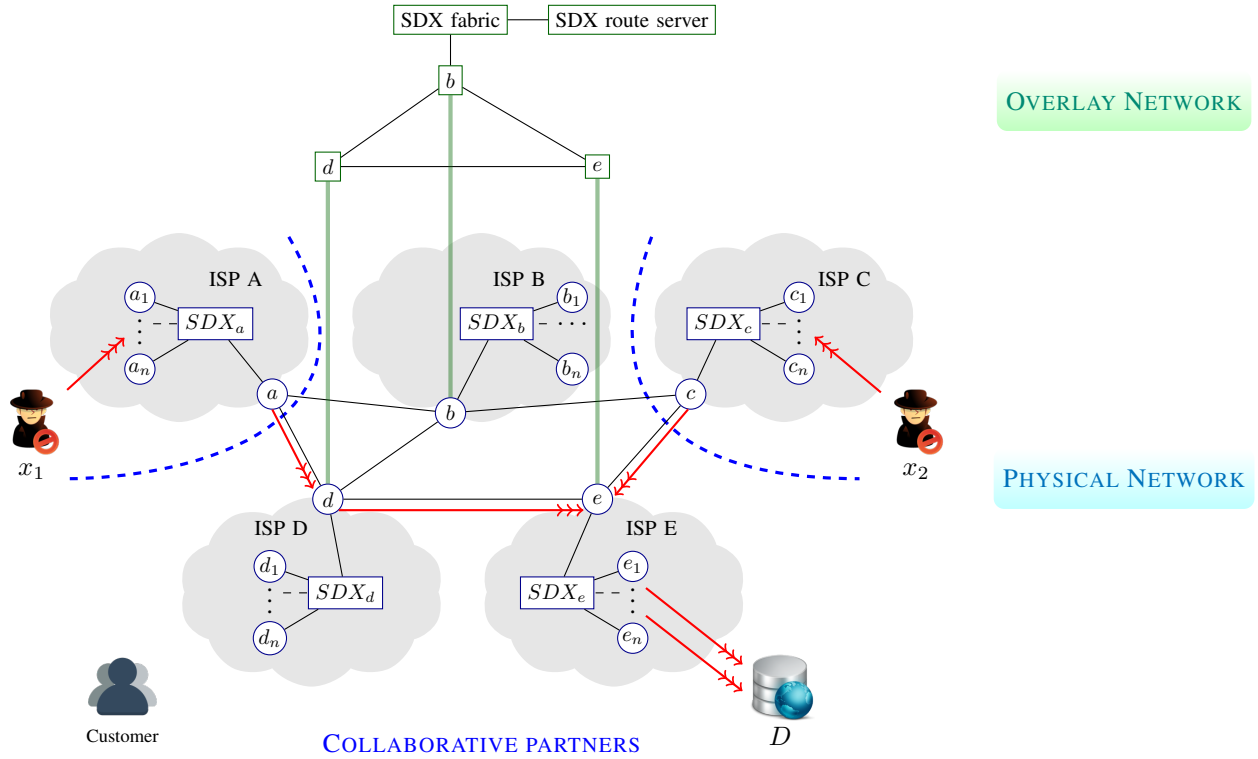


Fig. 1. A semantic representation of the testbed

V. DDoS Defense solution

In this section, we describe the main components of our proposed DDoS Defense solution and how these components interact with each other.

Our DDoS defense solution consists of multiple ISP networks as shown in Figure 1 and deploy the elements of (i) a typical flow monitoring setup, (ii) establish the exchange of security events and (iii) make use of a collaboration process, (iv) implement SDX as described in Section III-A.

In order to make use of a moving-target defense strategy, our DDoS defense solution combines the use of SDX and MTD. As a consequence, our approach of MTD is implemented using ONOS, a carrier-grade SDN network operating system. The advantage of using ONOS is that it ensures scalability by design as it has been used and tested in several high-speed networks.

Our DDoS Defense solution performs network-level MTD and host-level MTD [17]. The network-level MTD strategy is based on different BGP routes and multiple routers. The border router acts as a dispatcher while multiple routers are available on demand and are setup to change the shape of the network. The BGP routes are established and tested using Quagga[1]. In addition, our DDoS defense solution performs host-level MTD and performs IP-hopping in order to set up a honeypot.

A consistent and valid network configuration is ensured by a predefined set of valid network routes. The Adaptation Selection and Timing problem is beyond the scope of this paper as described in Section II-A.

[1]http://www.nongnu.org/quagga/

VI. Evaluation

In this section, we describe the qualitative and quantitative evaluation of the MTD using SDN in order to limit the effects of large-scale cyber attacks. First, we describe the characteristics of the evaluation criteria. Second, we introduce 9 evaluation criteria for the DDoS defense solution. Finally, we present and summarize the results of the evaluation.

A. Evaluation methodology

The collaborative DDoS defense solution is evaluated based on the following 9 criteria: Diversification, Adaptations, Randomization, MTD Entropy, Ease of Deployment, Timeliness, Scalability, Wide-area load balancing and Cost-conscious. These criteria were derived from the requirements described in Section III-B.

The criterion 'Diversification' describes the ability to select and use one network configuration out of multiple network configuration choices. The criterion 'Adaptations' refers to the ability to support movements within the system that do not change the shape of the network graph and also support transformations that change the size and shape. The Unpredictability of the movements and transformations of the selected network configuration is described by the criterion 'Randomization'. The effectiveness of a chosen MTD strategy is measured by using the MTD entropy and thus as higher the MTD entropy value, the better the effectiveness of a MTD

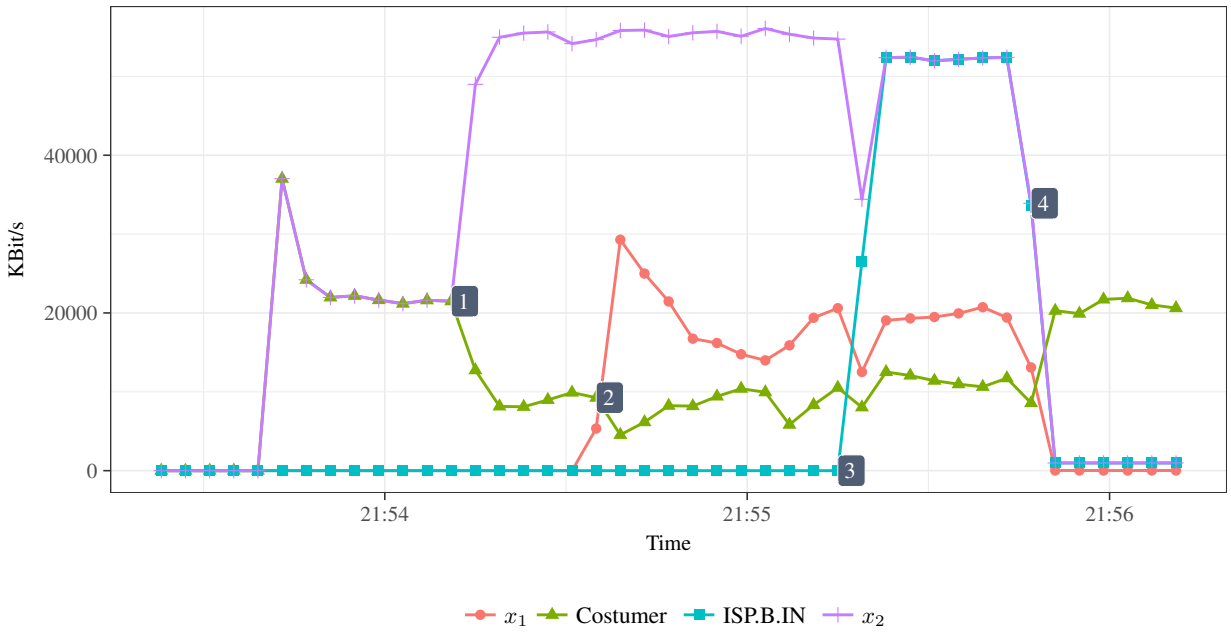


Fig. 2. Qualitative evaluation results

strategy. The criterion 'Ease of Deployment' describes the ability to use the DDoS defense solution and its underlying implementation on different operating systems, infrastructure devices and network protocols. The criterion 'Timeliness' refers to the ability to perform adaptations of the network configuration in an appropriate amount of time. The ability to support hundreds of collaborating partners, handle hundreds of thousands of IP prefixes and matching rules is described by the 'scalability' criterion. The 'wide-area load balancing' criterion describes the ability to divert malicious traffic into a network of collaborating partners and forward it to a scrubber or honeynet for further analysis. The costs to run and deploy a DDoS defense solution using MTD and SDN are described by the criterion 'cost-conscious'.

B. Qualitative Evaluation Results

In this section, we present the results of a qualitative evaluation of the DDoS defense solution using MTD and SDN.

a) Ease of Deployment: The heterogeneity of network devices and used operating systems requires a platform independent DDoS defense solution that easily integrates within the existing infrastructure. Therefore, the implementation of our DDoS defense solution is based on Open Network Operating System (ONOS). ONOS is written in Java and provides a distributed SDN applications platform atop Apache Karaf OSGi container and thus can easily be deployed on different operating systems. Further, the DDoS defense solution is composed of hardware that supports the OpenFlow communications interface as a study of Steinberger et al. [13] revealed that the majority of network operators plan or consider to have the technical ability to use OpenFlow in the near future.

b) Scalability: The DDoS defense solution is scalable by design as it based on ONOS and SDX. ONOS is designed for performance, high availability, scale-out and well-defined northbound and southbound abstractions and interfaces [33]. Further, ONOS is gaining momentum around WAN use cases for service providers and is backed by AT&T, Ciena, Cisco, Ericsson, Fujitsu, Huawei, Intel, NTT, NEC, SK Telecom, and many others [33]. Besides, ONOS and OpenFlow, we make use of SDX that ensures an appropriate rule-table size and network broadcast overhead. As a result, our DDoS defense solution interoperates with large, heterogeneous environments.

c) Cost-conscious: A study of Steinberger et al. [13] investigated the technical ability to use SDN to be able to deploy a constantly adapting environment. The majority of network operators plan or consider to have the technical ability to use SDN (e.g., OpenFlow) in the near future. Therefore our approach can be easily deployed within the existing network infrastructure. Further, the costs of a DDoS defense solution depends on time-of-use of resources and bandwidth-based network resources. As our solution focuses on collaboration of trusted partners to mitigate large-scale cyber attacks, expertise and available resources are bundled and thus a smaller amount of resources and bandwidth is required to identify and mitigate ongoing attacks. As a result, our DDoS solution is cost-conscious.

C. Quantitative Evaluation

In this section, we perform a quantitative evaluation of the DDoS defense solution using MTD and SDN. First, we describe the setup of our testbed. Second, we present the test scenario of our DDoS defense solution.

1) Setup of the testbed: Mininet [34] is a network emulation orchestration system designed for lightweight virtualization of a complete network. We used Mininet and ONOS to evaluate our DDoS defense solution. The experiment is composed of virtual hosts, switches, links, and controllers. Mininet is used because it is a controlled environment in which it is possible to safely test security threats and defense measures. Our DDoS defense solution consists of 5 nodes representing Internet Service Providers (ISP $A - E$) connected through a link. In each ISP network, SDX is deployed and is installed as shown in Figure 1. In addition, the ISP networks B, D and E are collaborative partners and share security events using the communication process described [10]. Figure 1 shows a schematic representation of our Mininet testbed.

2) Test scenario: The objective of the experiments is to show that a target network with constrained resources benefits from the use of an MTD strategy during an ongoing network-based attack, because a dynamic shift of the attack surface increases the uncertainty and apparent complexity for the attacker. Further, we show that the large-scale cyber attack is not propagated further through the ISP networks and that the use of an MTD strategy combined with an collaborative approach appropriately limits their effects.

To simulate a large-scale cyber attack, we performed a distributed TCP SYN flood attack from the ISP networks A and C to consume resources on the web server within ISP network E and render it unresponsive as shown in Figure 1. In our test scenario, the detection engine of the ISP network E initially identifies the malicious network traffic targeting its network and initiates an MTD strategy that changes the attack surface. Next, the ISP E informs its trusted collaborating partners about the changes and as a result the partners also start to change their networks. To create the TCP SYN flood attack, we used empty TCP packets with a TCP packet size of 40 bytes and a TCP FLAGS value of $0x02$.

Based on the test scenario, we perform two experiments. The result of the experiments are shown in Figure 2. First, attacker x_2 who resides in ISP network C launches the TCP SYN flood attack targeting the web server within ISP network E using the network path $c \rightarrow e$. At the same time, we assume the occurrence of benign traffic in each ISP network. In particular, we placed a benign customer within ISP network D that tries to access the web server within ISP network E using the network path $d \rightarrow e$. In Figure 2, we show that a customer in ISP network D faces service degradation in form of less bandwidth availability as a result of the TCP SYN Flood (1). Next, attacker x_1 in ISP network A launches the TCP SYN flood attack targeting the web server in ISP network E using the network path $a \rightarrow d \rightarrow e$ (2). As a result, the customer in ISP network D faces another service degradation in form of less bandwidth availability. In the meantime, the collaborative partners exchanged security events initiated by ISP network E using the communication process described in [10] and use MTD.

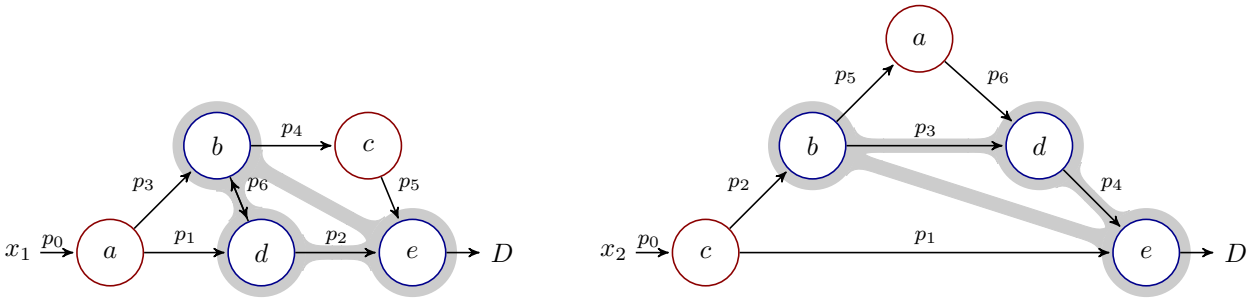
In our first experiment, ISP network D splits up the occurring network traffic into benign and malicious traffic and reroutes the malicious network traffic to the network of collaborative partners. The reason is that high-speed networks have redundant link capacities in place and their average link utilization is less than 30% [35], [36]. Therefore, the collaborative DDoS defense solution bundles resources of all collaborating partners to handle the amount of malicious network traffic and ensure availability. As a result, the malicious network traffic from the attacker x_1 is rerouted and using the network path $a \rightarrow b \rightarrow c \rightarrow e$ (3). Further, the network path $d \rightarrow e$ recovers and provides slightly more bandwidth to the customer in ISP network D. Finally, ISP network E changes the attack surface using MTD, adds an additional network path and deploys various link capacities to the web server D. As shown in Figure 2, ISP E also splits up the incoming traffic into benign and malicious traffic. The malicious traffic is rerouted over a rate-limited link to the web server and thus the available bandwidth of the customer in ISP network D recovers (4).

3) Quantitative Evaluation Results: In this section, we present the results of a quantitative evaluation results of the DDoS defense solution using MTD and SDN.

a) Diversification: Within an ISP network multiple configuration choices are available. The number of configuration choices increase, as larger the ISP network. In our test scenario, we consider one virtual host (customer), multiple routers, links, link capacities and controllers available in the configuration space. ONOS provides the capability to switch between different configuration choices by using the ONOS API and enhance the functionality with a custom ONOS application.

b) Adaptations: Adaptations are used within the collaborative ISP network to transform the collaborative ISP network from one configuration state s into another valid configuration state s. As emerged from the test scenario, we perform three adaptations: increase uncertainty and apparent complexity through the establishment of alternative routes within α_1 the network of collaborating partners or α_2 within the network of a single ISP and α_3 change the configuration state s of the link capacity within ISP network E. The adaptations of our test scenario are deployed using ONOS. The effects of the deployment of the adaptation are visualized in Figure 2. In particular, adaptation α_1 was deployed in 3, adaptation α_2 and α_3 were deployed in 4. Figure 2 shows that the adaptations limit the effects of the TCP SYN flood and thus contribute to ensure availability of the organization's network infrastructure.

c) Randomization: In our experiment, the set S of the configuration states of the MTD systems consist of all possible network paths, rerouting of network traffic within the network of collaborating partners or in each ISP network and rate-limiting on all available links. Further, host configuration parameters e.g., IP addresses, operating systems, memory configurations are also part of the configuration space s. For reasons of simplicity, Figure 2 does not consider host configuration parameters. However, ONOS offers an API to customize the ONOS functionality. Even though ONOS does not provide configuration randomization from scratch, it provides the capability to enhance its functionality by own



(a) Attacker x_1 (b) Attacker x_2

Fig. 3. Transition model of attacker x_1 and x_2

scripts and thus provides the capability to randomly select the next configuration state to ensure unpredictability.

d) MTD Entropy: The attackers x_1 and x_2 try to render target D (an http web server) unresponsive. The attack is going through the network of ISP E though multiple available network paths as shown in Figure 3. The values p_i where $i = \{0 \leq i \leq 6 | i \in \mathbb{N}_0\}$ represent the transition probabilities from x_1 to D that include the possibility of MTD adaptation. We adhere to the probability calculations defined in [14] and adapt these to the scenario described in III-A. In contrast to Zhuang et al. [14], we only consider forward transitions which represent the *hot-potato routing* [37]. Hot-potato routing refers to the selection of the closest egress point, the router with the smallest intradomain distance, when more than one route to the destination exist. Further, we consider that ISP network A and C are not using MTD and thus are not adapting. The ISP networks B, D and E are collaborative partners, exchange security events using a communication process as described in [10] and make use of MTD. From the perspective of the attacker x_1 the shortest path to the target D is the network path $a \rightarrow d \rightarrow e$. As the network of ISP D, ISP E and the target D make use of MTD, we consider $2^3 = 8$ different configuration states S. From the perspective of the attacker x_2 the shortest path to the target D is the network path $c \rightarrow e$. As the network of ISP E and the target D make use of MTD, we consider $2^2 = 4$ different configuration states S. We assume the attackers x_1 and x_2 are limited to valid communication paths, know those paths, continue diligently to send traffic to the target D and try to avoid using paths of the other attacker network to not weaken the amount of attack traffic reaching the target D. Further, we assume that the adaptations available on the nodes of the collaborative partners ensure the enlargement of constrained resources and thus the effects of a DDoS attack are limited.

$$adapted = \left(\frac{k}{n}\right)^{\frac{Ta}{Tr}}; \qquad \overline{adapted} = \left(1 - \frac{k}{n}\right)^{\frac{Ta}{Tr}} \tag{2}$$

$$successful = \Big(1 - (1-p)\Big)^{\frac{Tr}{Ta}}; \quad \overline{successful} = \Big(1 - p\Big)^{\frac{Tr}{Ta}} \tag{3}$$

Example: Based on the formula (2) and formula (3) the probability P_D of a successful DDoS attack is calculated. To calculate the probability P_D of a successful DDoS attack from attacker x_1 to the target D, the multiplication of all probabilities of all possible path to the target are used as shown in formula (4).

$$P_D = \prod_{i=0}^{2} p_i \tag{4}$$

The ISP A network is not using MTD and thus is not adapted during an ongoing DDoS attack. Therefore, the probability is shown in formula (5).

$$p_0 = \left(1 - \frac{k}{n}\right)^{\frac{Ta}{Tr}} \tag{5}$$

As the network of ISP D and E are collaborative partners, and make use of MTD their networks may get adapted during an ongoing attack. In case the network of ISP D is not adapted during the ongoing attack, the DDoS attack is successful and saturates the constrained resources. This results in a probability shown in formula (6). In contrast, the network of ISP D is adapted during the ongoing attack and thus the effects of a DDoS attack mitigated. This results in a probability shown in formula (7).

$$p_{1a} = \Big(1 - (1-p)\Big)^{\frac{Tr}{Ta}} \cdot \left(1 - \frac{k}{n}\right)^{\frac{Ta}{Tr}} \tag{6}$$

$$p_{1b} = \Big(1 - p\Big)^{\frac{Tr}{Ta}} \cdot \left(\frac{k}{n}\right)^{\frac{Ta}{Tr}} \tag{7}$$

As the network of ISP E also make use of MTD, the probabilities of p_{2a} and p_{2b} remain the same as presented in formula (6) and (7). Next, the target D within the network of ISP E also may get adapted. This results in a probability shown in formula (8) and (9).

$$p_{3a} = \left(\frac{k}{n}\right)^{\frac{Ta}{Tr}} \tag{8}$$

$$p_{3b} = \left(1 - \frac{k}{n}\right)^{\frac{Ta}{Tr}} \tag{9}$$

As reported in [38], the average DDoS attack duration is 58 minutes and the number of attacks experienced per month is

TABLE I
OVERALL PROBABILITY P_D OF A SUCCESSFUL DDOS ATTACK OF 8 CONFIGURATION STATES s

#	ISP D	ISP E	target D	P_D
1	$adapted$	$adapted$	$adapted$	2.2301×10^{-7}
2	$adapted$	$\overline{adapted}$	$adapted$	5.0984×10^{-6}
3	$adapted$	$adapted$	$\overline{adapted}$	6.3730×10^{-7}
4	$adapted$	$\overline{adapted}$	$\overline{adapted}$	1.4570×10^{-5}
5	$\overline{adapted}$	$adapted$	$adapted$	6.3730×10^{-7}
6	$\overline{adapted}$	$\overline{adapted}$	$adapted$	1.4570×10^{-5}
7	$\overline{adapted}$	$adapted$	$\overline{adapted}$	1.8212×10^{-6}
8	$\overline{adapted}$	$\overline{adapted}$	$\overline{adapted}$	4.1635×10^{-5}

more than 21. As a consequence, we set the Attack Interval $\mathrm{Ta} = 60\,\mathrm{min}$. In accordance to the MTD Adaptation Interval selected by [14], the Adaptation Interval is set to $\mathrm{Tr} = 20\,\mathrm{min}$ and the number of adaptations is set to $k = 1$. The overall probability P_D of a successful DDoS attack of 8 configuration states is listed in Table I. As shown in Table I the overall probability P_D of a successful DDoS attack decreases as more collaborative ISP networks process the network traffic and make use of MTD.

e) Timeliness: The primary focus to mitigate and respond to network-based attacks is maintaining the availability of the organization's network infrastructure and services. Therefore, the DDoS defense solution performs several adaptations to increase uncertainty and apparent complexity for the attackers. As shown in Figure 2, the adaptations (label 3 and 4) are deployed and their effects are immediately visible (more available bandwidth for the customer located in ISP network D).

f) Wide-area load balancing: In [35], [36], the authors reported that high-speed networks have redundant link capacities in place and their average link utilization is less than 30%. As a consequence, wide-area load balancing should be used to mitigate and respond to large-scale cyber attacks. In our test scenario, the collaborating partners bundle resources in order to mitigate and respond to large-scale cyber attacks. Further, the collaborating networks diversify the amount of malicious traffic among all collaborating partners to ensure availability of the organization's infrastructure. Moreover, wide-area load balancing among collaborative networks provides the possibility to analyze the attacker's behavior. ONOS provides the capability to perform wide-area load balancing.

VII. CONCLUSION

Distributed large-scale cyber attacks pose a serious threat to the network infrastructure and services. One approach to mitigate and respond to large-scale cyber attacks is to move as close to the source of the attack as possible and thus move to the network of Internet Service Providers.

In this paper, we investigated the effectiveness of the defense technique moving target using Software Defined Networking in an collaborative environment in context of Internet Service Providers. In particular, we focused on the Software Defined Networking OS called ONOS.

We have shown that the overall probability of a successful DDoS attack decreases as more collaborative partners process the network traffic and make use of MTD. Further, we found that ONOS is an appropriate Software Defined Networking OS to enforce implementation of the moving target defense to mitigate the effects caused by large-scale cyber attacks. In addition, we have shown that a moving target defense strategy significantly reduces the effects of a large-scale cyber attack.

To overcome closed source and system dependency of this research domain, we share the test scenario scripts as public available data which can be downloaded from https://www.dasec.h-da.de/staff/jessica-steinberger.

ACKNOWLEDGMENT

This work was partly supported by the German Federal Ministry of Education and Research (BMBF), the Hessen State Ministry for Higher Education, Research and the Arts (HMWK) within the Center for Research in Security and Privacy (CRISP) and by the Netherlands Organisation for Scientific Research (NWO) Distributed Denial-of-Service Defense: Protecting Schools and other public organizations (D3) Project.

REFERENCES

[1] B. Krebs. (2016) KrebsOnSecurity Hit With Record DDoS. Website. [Online]. Available: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

[2] Akamai Technologies. (2016) akamai's [state of the internet]/security: Q3 2016 report. Website. [Online]. Available: https://www.akamai.com/uk/en/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp

[3] B. Krebs. (2016) New Mirai Worm Knocks 900K Germans Offline. Website. [Online]. Available: https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/

[4] B. Schneier. (2016, Nov) Corporate Responsibility - Lessons from the Dyn DDoS Attack. Website. [Online]. Available: https://www.telekom.com/en/corporate-responsibility/data-protection---data-security/magenta-security-congress-2016/magenta-security-congress-2016/lessons-from-the-dyn-ddos-attack-444586

[5] J. J. Santanna, R. van Rijswijk-Deij, R. Hofstede, A. Sperotto, M. Wierbosch, L. Zambenedetti Granville, and A. Pras, "Booters - An analysis of DDoS-as-a-service attacks," in *Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management 2015 (IM 15)*, May 2015, pp. 243–251.

[6] C. Cimpanu. (2016) You Can Now Rent a Mirai Botnet of 400,000 Bots. Website. [Online]. Available: https://www.bleepingcomputer.com/news/security/you-can-now-rent-a-mirai-botnet-of-400-000-bots/

[7] R. Zhuang, S. A. DeLoach, and X. Ou, "Towards a Theory of Moving Target Defense," in *Proceedings of the First ACM Workshop on Moving Target Defense*, ser. MTD '14. New York, NY, USA: ACM, 2014, pp. 31–40. [Online]. Available: http://doi.acm.org/10.1145/2663474.2663479

[8] R. Zhuang, A. G. Bardas, S. A. DeLoach, and X. Ou, "A Theory of Cyber Attacks: A Step Towards Analyzing MTD Systems," in *Proceedings of the Second ACM Workshop on Moving Target Defense*, ser. MTD '15. New York, NY, USA: ACM, 2015, pp. 11–20. [Online]. Available: http://doi.acm.org/10.1145/2808475.2808478

[9] Cloudflare, Inc. (2016) Cloudflare Pricing. Website. [Online]. Available: https://www.cloudflare.com/plans/

[10] J. Steinberger, B. Kuhnert, A. Sperotto, H. Baier, and A. Pras, "Collaborative DDoS defense using flow-based security event information," in *Proceedings of the IEEE/IFIP Network Operations and Management Symposium 2016 (NOMS 16)*, Apr 2016, pp. 516–522.

[11] H. Okhravi, T. Hobson, D. Bigelow, and W. Streilein, "Finding focus in the blur of moving-target techniques," *IEEE Security Privacy*, vol. 12, no. 2, pp. 16–26, Mar 2014.

[12] A. Gupta, L. Vanbever, M. Shahbaz, S. P. Donovan, B. Schlinker, N. Feamster, J. Rexford, S. Shenker, R. Clark, and E. Katz-Bassett, "SDX: A Software Defined Internet Exchange," *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 4, pp. 579–580, Aug 2014. [Online]. Available: http://doi.acm.org/10.1145/2740070.2631473

[13] J. Steinberger, A. Sperotto, H. Baier, and A. Pras, "Collaborative attack mitigation and response: A survey," in *IFIP/IEEE International Symposium on Integrated Network Management (IM)*, May 2015, pp. 910–913.

[14] R. Zhuang, S. A. DeLoach, and X. Ou, "A Model for Analyzing the Effect of Moving Target Defenses on Enterprise Networks," in *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, ser. CISR '14. New York, NY, USA: ACM, 2014, pp. 73–76. [Online]. Available: http://doi.acm.org/10.1145/2602087.2602088

[15] F. Chong, R. B. Lee, C. Vishik, A. Acquisti, W. Horne, C. Palmer, A. K. Ghosh, D. Pendarakis, W. H. Sanders, E. Fleischman, H. Teufel III, G. Tsudik, D. Dasgupta, S. Hofmeyr, and L. Weinberger. (2009) National Cyber Leap Year Summit 2009 Co-Chairs' Report . Website. [Online]. Available: https://www.nitrd.gov/nitrdgroups/images/b/bd/National_Cyber_Leap_Year_Summit_2009_CoChairs_Report.pdf

[16] E. Rhyne. Moving Target Defense. Website. [Online]. Available: https://www.dhs.gov/science-and-technology/csd-mtd

[17] Morphisec Ltd. (2016) Moving Target Defense: Common Practices. Website. [Online]. Available: http://blog.morphisec.com/moving-target-defense-common-practices

[18] O. N. Foundation, "Software-defined networking: The new norm for networks," ONF White Paper, ONF White Paper, Apr. 2012.

[19] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: Enabling innovation in campus networks," *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, Mar. 2008.

[20] R. Hofstede, P. Čeleda, B. Trammell, I. Drago, R. Sadre, A. Sperotto, and A. Pras, "Flow Monitoring Explained: From Packet Capture to Data Analysis With NetFlow and IPFIX," *IEEE Communications Surveys Tutorials*, vol. 16, no. 4, pp. 2037–2064, May 2014.

[21] C. Morrow and R. Dobbins. (2015, Jul) DDoS Open Threat Signaling (DOTS) Working Group Operational Requirements. Website. [Online]. Available: https://www.ietf.org/proceedings/93/slides/slides-93-dots-3.pdf

[22] R. Wang, D. Butnariu, and J. Rexford, "OpenFlow-based Server Load Balancing Gone Wild," in *Proceedings of the 11th USENIX Conference on Hot Topics in Management of Internet, Cloud, and Enterprise Networks and Services*, ser. Hot-ICE'11. Berkeley, CA, USA: USENIX Association, 2011, pp. 1–6. [Online]. Available: https://www.usenix.org/conference/hot-ice11/openflow-based-server-load-balancing-gone-wild

[23] H. Wang, F. Li, and S. Chen, "Towards cost-effective moving target defense against ddos and covert channel attacks," in *Proceedings of the 2016 ACM Workshop on Moving Target Defense*, ser. MTD '16. New York, NY, USA: ACM, 2016, pp. 15–25. [Online]. Available: http://doi.acm.org/10.1145/2995272.2995281

[24] Q. Jia, K. Sun, and A. Stavrou, "MOTAG: Moving Target Defense against Internet Denial of Service Attacks," in *22nd International Conference on Computer Communication and Networks (ICCCN)*, Jul 2013, pp. 1–9.

[25] H. Wang, Q. Jia, D. Fleck, W. Powell, F. Li, and A. Stavrou, "A moving target DDoS defense mechanism," *Computer Communications*, vol. 46, pp. 10 – 21, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366414000954

[26] Q. Jia, H. Wang, D. Fleck, F. Li, A. Stavrou, and W. Powell, "Catch Me If You Can: A Cloud-Enabled DDoS Defense," in *44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, Jun 2014, pp. 264–275.

[27] S. Venkatesan, M. Albanese, K. Amin, S. Jajodia, and M. Wright, "A Moving Target Defense Approach to Mitigate DDoS Attacks against Proxy-Based Architectures," in *IEEE Conference on Communications and Network Security 2016*, Oct 2016.

[28] M. Wright, S. Venkatesan, M. Albanese, and M. P. Wellman, "Moving target defense against ddos attacks: An empirical game-theoretic analysis," in *Proceedings of the 2016 ACM Workshop on Moving Target Defense*, ser. MTD '16. New York, NY, USA: ACM, 2016, pp. 93–104. [Online]. Available: http://doi.acm.org/10.1145/2995272.2995279

[29] D. C. MacFarland and C. A. Shue, "The SDN Shuffle: Creating a Moving-Target Defense Using Host-based Software-Defined Networking," in *Proceedings of the Second ACM Workshop on Moving Target Defense*, ser. MTD '15. New York, NY, USA: ACM, 2015, pp. 37–41. [Online]. Available: http://doi.acm.org/10.1145/2808475.2808485

[30] S. Debroy, P. Calyam, M. Nguyen, A. Stage, and V. Georgiev, "Frequency-minimal moving target defense using software-defined networking," in *Proceedings of the 2016 International Conference on Computing, Networking and Communications (ICNC)*, Feb 2016, pp. 1–6.

[31] A. Chowdhary, S. Pisharody, and D. Huang, "Sdn based scalable mtd solution in cloud network," in *Proceedings of the 2016 ACM Workshop on Moving Target Defense*, ser. MTD '16. New York, NY, USA: ACM, 2016, pp. 27–36. [Online]. Available: http://doi.acm.org/10.1145/2995272.2995274

[32] B. Ager, N. Chatzis, A. Feldmann, N. Sarrar, S. Uhlig, and W. Willinger, "Anatomy of a Large European IXP," *ACM SIGCOMM Computer Communication Review*, vol. 42, no. 4, pp. 163–174, Aug 2012. [Online]. Available: http://doi.acm.org/10.1145/2377677.2377714

[33] SDNCentral LLC. (2016) The Future of Network Virtualization and SDN Controllers. Website. [Online]. Available: https://www.sdxcentral.com/reports/network-virtualization-sdn-controllers-2016/

[34] B. Lantz, N. Handigol, B. Heller, and V. Jeyakumar. (2016) Introduction to Mininet. Website. [Online]. Available: https://github.com/mininet/mininet/wiki/Introduction-to-Mininet

[35] T. Otoshi, Y. Ohsita, M. Murata, Y. Takahashi, K. Ishibashi, and K. Shiomoto, "Traffic prediction for dynamic traffic engineering," *Computer Networks*, vol. 85, pp. 36 – 50, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128615001565

[36] A. Hassidim, D. Raz, M. Segalov, and A. Shaqed, "Network utilization: The flow view," in *In Proceedings of the IEEE INFOCOM*, April 2013, pp. 1429–1437.

[37] R. Teixeira, A. Shaikh, T. G. Griffin, and J. Rexford, "Impact of Hot-Potato Routing Changes in IP Networks," *IEEE/ACM Transactions on Networking*, vol. 16, no. 6, pp. 1295–1307, Dec 2008.

[38] Arbor Networks. Worldwide Infrastructure Security Report. Website. [Online]. Available: https://www.arbornetworks.com/insight-into-the-global-threat-landscape