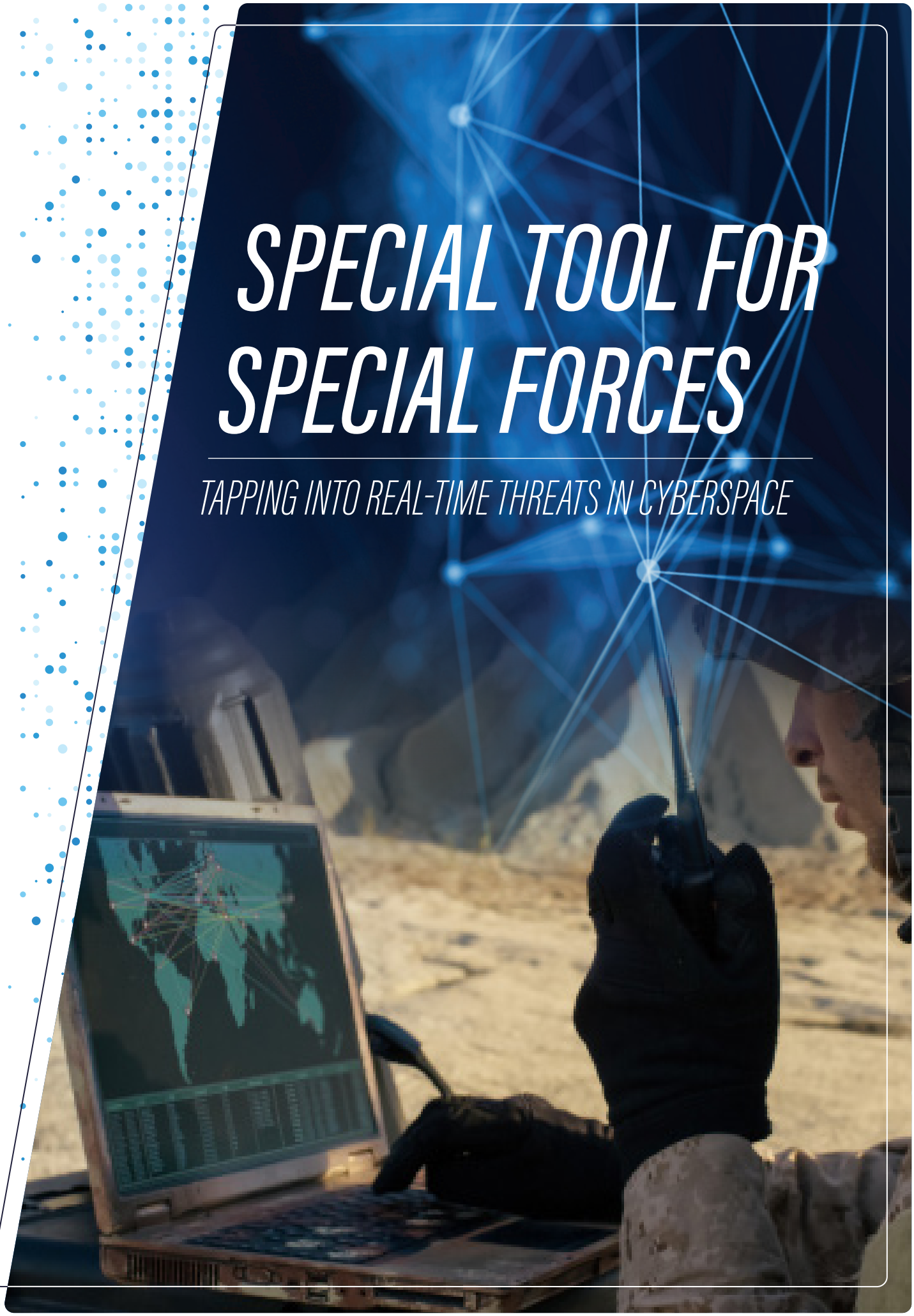
SPECIAL TOOL FOR SPECIAL FORCES

TAPPING INTO REAL-TIME THREATS IN CYBERSPACE



CYBERSECURITY: A RISING CHALLENGE

Security is one of the biggest concerns in our society today. Since the turn of the 21st Century, the world has faced many challenges in maintaining the security of its people, economy and infrastructure. The biggest concern in this new digital age, is information security, commonly referred to as cybersecurity. Due to ever evolving technological advancements and sophisticated threat mechanisms, the vulnerability of the cyber world is greater than ever before. Traditional crimes are now being vectored through cyberspace, such as public attacks, financial fraud, compromise of security intelligence information, and even penetration into national defense communications. All of these bear significant economic and humanitarian consequences. With the reliance of information technology increasing in our every day lives, the risk of security violation is also increased.

Cyberspace is intangible, making it harder to secure than the physical world. Yet this makes it easier to threaten, and attack. Cybersecurity has become a priority for defense forces and law enforcement agencies worldwide. The severity of potential threats has seen the creation of special purpose technical security teams within these bodies, to maximize the safety of their information security. These teams have varying roles, including network security and defense, post-event forensic analysis, hacking and penetration, security intelligence and surveillance, and on-field threat defense.

SEEING BEYOND THE NETWORK

Some manufacturers have introduced a basic version of their full-duplex TAP, and market it as their portable model. However these are small enough to cater to just one network link. Basically they are smaller versions of the rack-mount models and still contain rack-mount screw holders.

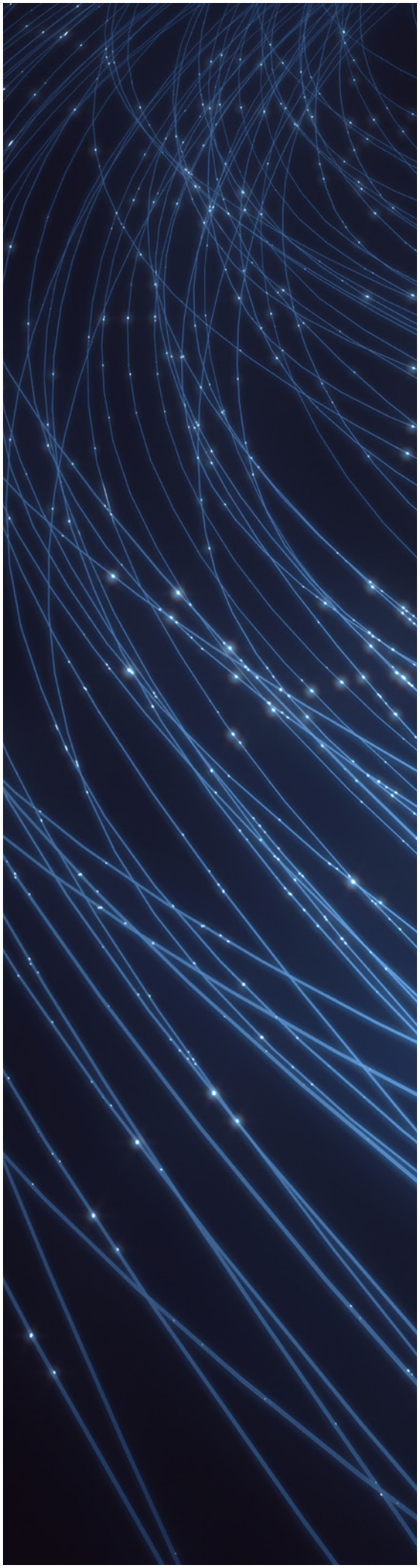
Being a full-duplex TAP, it does capture the traffic at full line-rate without any packet loss or timing delay. So the performance is there, but it is still difficult for an IT engineer to carry around a 'portable' TAP like this in the field, because additional hardware is required.

A full-duplex TAP, or Breakout TAP, captures traffic streams from two network ports and copies them onto two 'output' or monitoring ports. This is what complicates things in the field. Besides the full-duplex TAP itself, you also need to have a lunch-box PC containing dual network-interface cards (NIC). In addition to this, the PC hosting the monitoring application would also have to perform interface- bonding or link-aggregation, to 'see' the two interfaces as one single stream of traffic.

This means double the resources, double the cost, and double the time required to start your network analysis. Let's accept it – you can't carry a desktop around in field locations, and neither do you have dual NICs in your laptop. (How many companies dish out dual-NIC high-performance laptops to their field staff anyway?)

As you can see, portability on paper and portability in practice are two very different things when it comes to network TAPs.

The second, and more reliable method to capture packets is using a network TAP (Traffic Access Point). A TAP is a piece of hardware that is installed in-line on a network link. It creates an internal mirror of the traffic without disrupting it. It does not create any of the bottlenecks involved in using port-mirroring. TAP's guarantee full capture of 100% of packets from the live traffic in real-time, because a TAP captures packets on the wire. TAP's are used extensively in security applications because they are non-intrusive and are undetectable on the network. Having no physical or logical address, a cybersecurity team can execute their activity using a TAP in complete stealth mode.



SWAT-STYLE OPERATIONS IN THE CYBERSPACE

First established in the United States in 1964, Special Weapons and Tactics, or SWAT, is a term used by law enforcement agencies for security units that employ specialized equipment and tactics for handling threat defense and security operations. Unlike conventional responses, the prime objective of a SWAT force is to neutralize threats in real-time. Following the success of the SWAT force in the US, countries across the world have adopted this style of counter-terrorism.

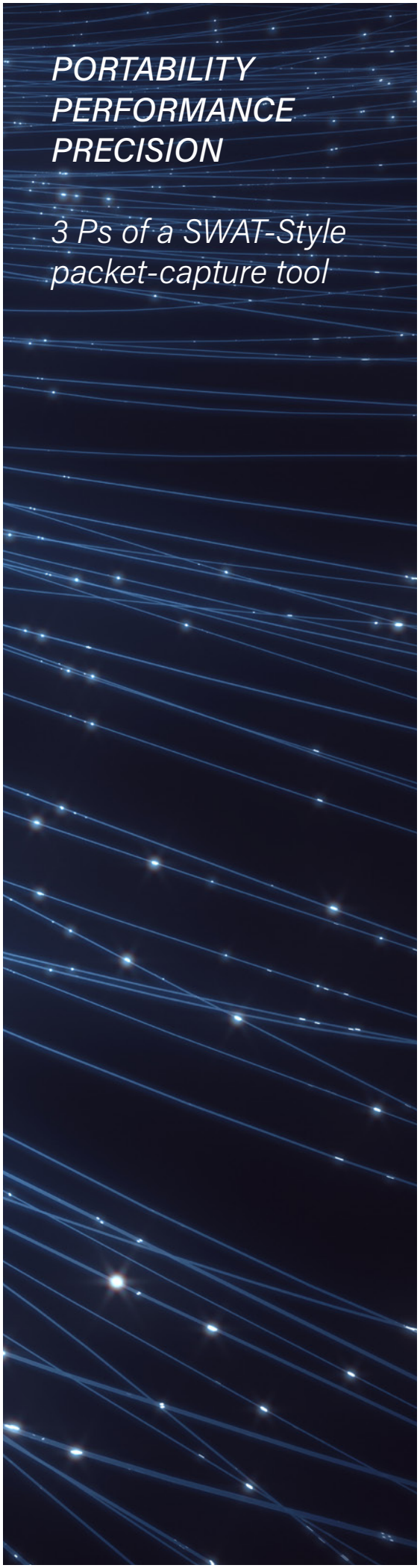
The key to a successful SWAT operation is choosing the right type of specialized equipment and deploying on-ground tactics based on the nature of the threat.

For cybersecurity teams to conduct their own SWAT-style operations in cyberspace, a tool which enables them to counter and neutralize threats in real-time is essential. Considering network TAP's to capture and analyze live traffic packets, the SWAT-style tool should have the following key characteristics.

Portability

Threats in cyberspace can originate from anywhere on the planet. DDoS attacks, hacking attempts, network penetration, malware exploitation, financial fraud – all of these events can be initiated from any location, even public places such as shopping malls, airports, or even hospitals. To counter these threats, special forces cybersecurity units either conduct on-ground surveillance on a periodic basis, or conduct raids at suspected locations. One of the quickest ways to uncover threats occurring in real-time is to capture and analyze packets flowing over backbone network links or uplinks serving internet to Wi-Fi access points.

A plug-&-play network TAP that can be installed instantly on network links, with the ability to scale up to Gigabit bandwidth, and which can be effortlessly plugged to a laptop, is the essential tool for the cybersecurity teams to quickly dive into the packets, and sniff the digital conversations in that location. Such a tool should be portable enough to be carried around on any field location and get installed in minutes without having to configure any aspect of the active network.



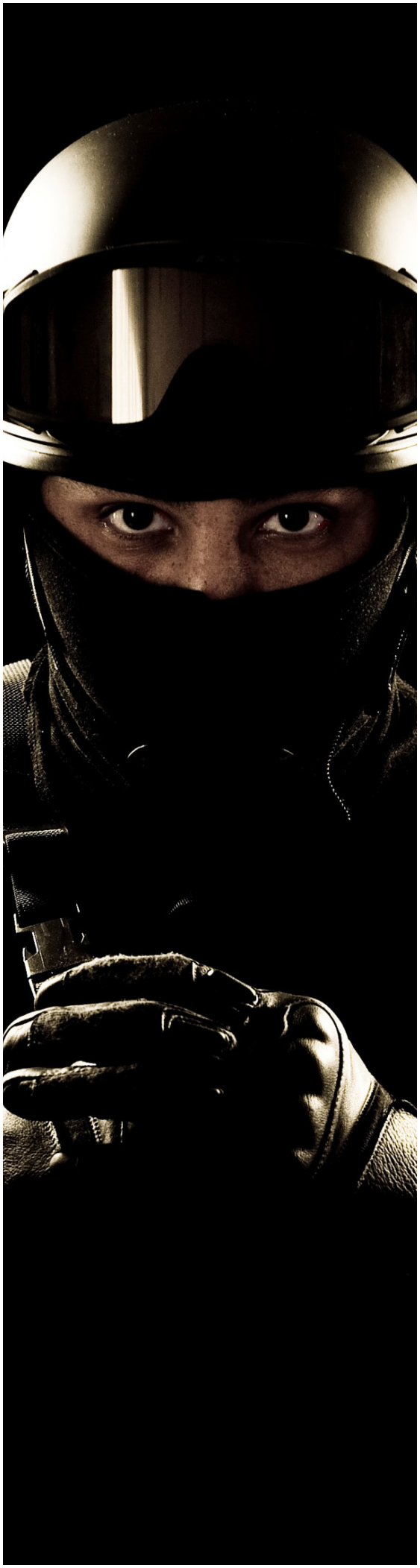
Performance

In addition to being portable, this tool should be powerful enough to capture 100% of traffic, without dropping any packets. The primary purpose of a TAP is to capture and analyse each and every packet, making it an ideal tool. How would the cybersecurity team be able to detect a threat if it does not receive all the packets in the first place? What if the critical packets, e.g. the ones containing the threat signature, or the defected hosts' address, or the originator's location identification, do not reach your packet analyser at all?

Network analyzers would not be able to reconstruct actual network flows if there are missing packets. Therefore when it comes to traffic monitoring and analysis, packet-drops are simply unacceptable. However, not all TAP's are good at capturing 100% of packets on the wire. Particularly if the network link is of Gigabit capacity, since both directions of the link (east and west) aggregate to a total of 2 Gbps of output stream in full duplex mode. To remain truly portable by being compatible with a laptop, the required network TAP needs to have a simple connection mechanism, and yet does not compromise on the ability to transfer all packets to the laptop through a wire speed of 2 Gbps or above.

Precision

In order to counter on-ground threats while they are happening, the cybersecurity team needs to react instantly. For this, they need to see the data flowing through the network in real-time. Being able to capture and correlate the packets in real-time is the key to ensure timely detection and suppression of cyber attacks. Even if a network TAP captures all the packets, it also needs to ensure that the packets contain the accurate timestamp, and get delivered in time for analysis. The difference between a successful cyber crime versus neutralizing the attack, is being able to detect and identify threats as they happens in real-time. Hence, the network TAP needs to have at least nanosecond precision built into its hardware to ensure the packets contain the actual time of their occurrence over the network.



SPECIAL TOOL FOR SPECIAL FORCES

In comes the world's best, fastest and truly portable network TAP ready for any kind of packet capture in any field location. ProfiShark1G is pocket-sized yet power-packed. It works as a packet capture tool without any dropped packets or time delay. With the 2 x Gigabit network ports, it easily aggregates the two traffic streams over a single monitoring port. The ProfiShark 1G does not use a Gigabit NIC as the monitoring port. Instead, it utilizes the power of USB 3.0. USB 3.0 is the third major revision of the Universal Serial Bus standard that uses a new transfer mode, SuperSpeed, which can transfer data at up to 5 Gbps. Hence it can easily transport 2 Gbps of aggregated traffic stream (1G from each direction) over a USB 3.0 link. This means that the buffer memory doesn't need to drop any packets, nor does it store packets long enough to impact their timing.

Because it can easily connect to your laptop's USB port, a major advantage of the plug-&-play ProfiShark1G is that it is not dependent on an external power source. Combined with a laptop, you have a truly portable and powerful packet capture and analysis kit, ready to use at any location without depending on a power source.

The ProfiShark 1G captures and transfers packets directly to any host computer's disk. All packets are captured in real-time with nanosecond time-stamping at hardware level on each packet as it enters the TAP. This allows real-time analysis of captured traffic with nanosecond resolution. Plus, it has the ability to capture any type of frame, be it VLAN, VXLAN, MPLS, etc., between 10 bytes and 10 Kilobytes. It also captures low level error frames, e.g. CRC errors, which makes it a perfect tool to perform troubleshooting even at the lowest level. Furthermore, ProfiShark1G is PoE (Power over Ethernet) compliant as well, allowing the network links to transport power to the network equipments without any hindrance. Thus cybersecurity or cyber-response teams within law enforcement agencies or the special forces, can use this special tool for any kind of on-field analysis. ProfiShark 1G is the new member of your cyber squad.

If you are interested in trying out this SWAT-style tool in field, then please contact us or visit our website for further details.

PROFITAP

DISCOVER PROFISHARK

Go to: www.profitap.com/profishark

IT ALL STARTS WITH VISIBILITY

PROFITAP

Profitap develops and manufactures hardware and software solutions that help you get complete access and visibility into your network. These network visibility solutions are designed with the security, forensics, deep packet capture and network & application performance monitoring sectors in mind.

Profitap network solutions help eliminate network downtime, add security to existing and new networks all over the world, assist in lawful interception applications and reduce network complexity. All of Profitap's network monitoring tools are highly performant, secure and user-friendly, and provide complete visibility and access to your network, 24/7.

As we are experts in our field, we have developed our products to set new standards in an industry where the definition of excellence is constantly being challenged. With more than 1,000 clients from 55 countries, Profitap has become a must-have solution or many important businesses, many of which are among Fortune 500 companies.

PROFITAP HQ B.V.
HIGH TECH CAMPUS 9
5656 AE EINDHOVEN
THE NETHERLANDS

sales@profitap.com
www.profitap.com

Profitap

@Profitap

profitap-international