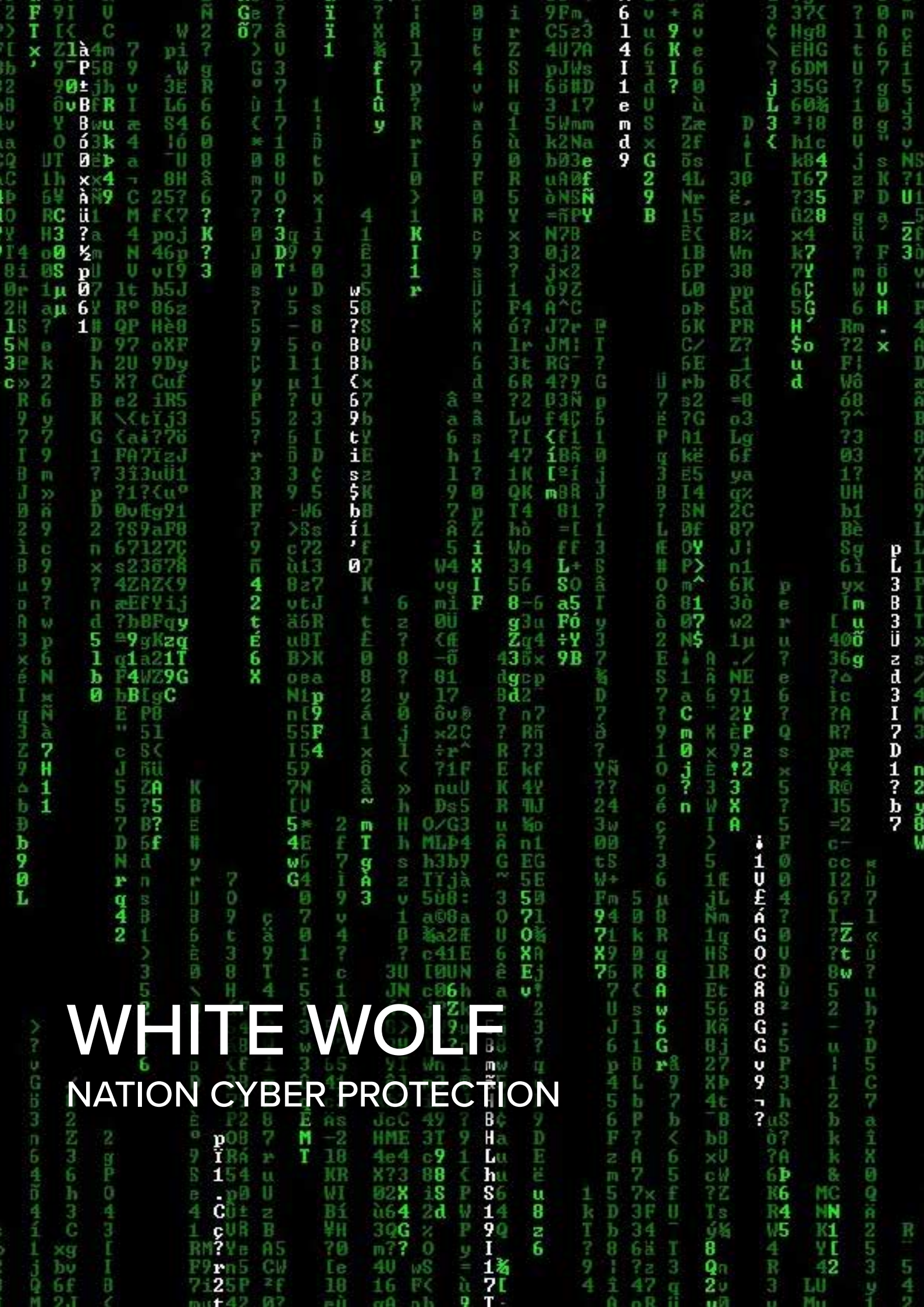

WHITE WOLF
NATION CYBER PROTECTION

FOREWORD

We live in a digital era, where cyber crime invasions and attacks flow in and out of a country like the wind passes through trees. No physical border fences, cctv cameras or military can stop this ever growing problem originate, enter or leave a country and the consequences can be catastrophic.

Over the years, the world has witnessed an increase of cyber attacks. In 2016, the global amount of data breaches and cyber attacks reached a record breaking 1.6 billion.

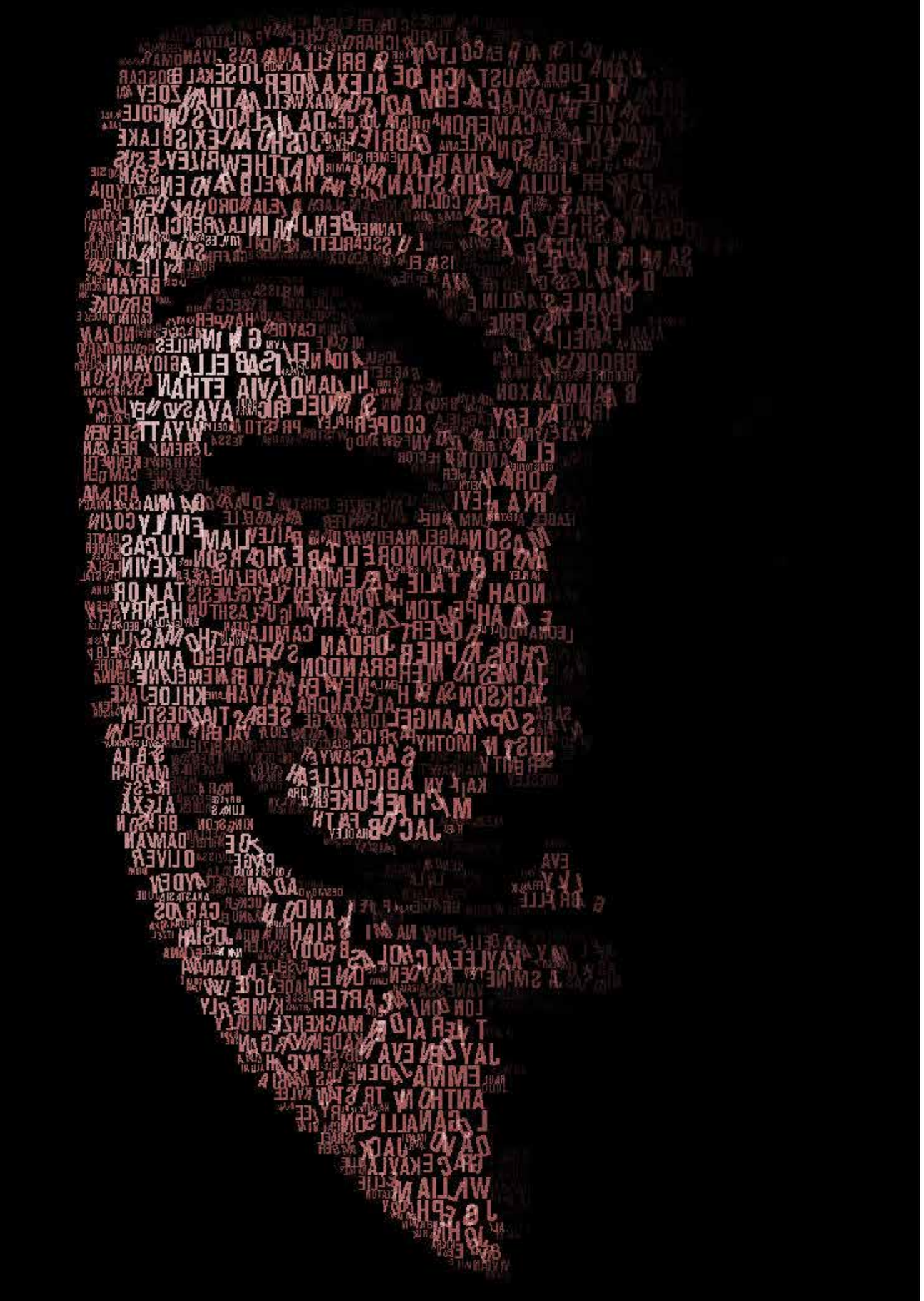
According to experts, cyber attacks is the biggest threat to mankind — even more of a bigger threat than nuclear weapons. From influencing elections in powerful nations to crippling entire corporations, cyber warfare is seeming to be much of a bigger threat than many have anticipated.

The global challenge of cyber crime has developed from an ‘emerging crime’ to a serious manifestation of crime with great practical relevance unique opportunities to connect with a global marketplace. In order to create both an enabling environment for enterprises and to protect users of Internet services in developing countries, it is necessary that countries have a clear legal framework and sufficient law enforcement and technological capacities in place to effectively fight cyber crime. Such frameworks and capacities are critical both to the protection of internet users within the country, and to the provision of effective support to foreign law enforcement agencies requesting international cooperation in cross national cyber crime cases.

There is a duty now for governments to defend every infrastructure asset, military, hospital, airport, oil refinery, university, church, telco, bank and human life from the threat of cyber crime. It is time to protect your country’s future.

Mak Chishty QPM

Former Commander at Metropolitan Police Service. Awarded the Queen’s Police Medal for Distinguished Service with 30 years of policing experience at the forefront of national and international policing.



GLOBAL CHALLENGE

With the emerging use of computer technology, computer related crimes have become a significant global challenge. The ability to automate attacks against computer systems can lead, for example, to hundreds of thousands of registered attempts to interfere with, or illegally access, computer systems each day.

Millions of computer viruses are detected every month and virus toolkits enable computer users with even limited skills to create malicious software. Through networks of literally millions of compromised computer systems controlled by individual criminal groups, even the most powerful Internet services can be attacked. Such threats are expensive, not only in terms of quantity, but also in terms of quality. In recent years, the number of reports concerning targeted attacks against critical infrastructure have increased. The Internet is based on single technical standards that allow global communication. This has the advantage of allowing the globalization of Internet services (such as Facebook, Google, Yahoo and others) that are operated in one country but can be accessed by users from all over the world.

From a crime prevention perspective, however, it has the disadvantage that acts of cybercrime do not require the offender to be located in the same country as the victim. This explains why the vast majority of cybercrime offences have a transnational dimension. Successful prevention and combating of cybercrime therefore requires effective international cooperation through adequate legal instruments and well trained government and law enforcement personnel. Although businesses in developed countries are often most affected by the abuse of Internet services to facilitate cyber crime, the topic is equally relevant for developing countries.

National assets are increasingly becoming a hotspot for cyber crime as organised criminals and terrorist groups increase their recruitment of cyber security talent in order to attack enemy infrastructure as part of their offensive strategy. This combined with strong calls for ‘political hacktivism’ has meant that cyber offensives are increasingly being resorted to where enemy groups struggle to maintain a strong physical presence in a target’s territory.

The country with highest number of malware-infected computers in the world is China. According to research, an estimated 57.24 percent of all computers in China are infected by malware. The runner up is Taiwan, with 49.15 percent of all computers infected, followed by Turkey with 42.52 percent of all computers infected.

The true cost of a security breach is potentially greater than any physical monetary loss: irretrievable sensitive data, employee time, disrupted focus, political ramifications, legal implications and damage to brand reputation. An ISACA survey to its members in 129 countries found that 83% viewed cyberattacks as one of the top three threats to businesses however only 38% felt prepared. How can organisations combat a cyber attack?

WHITE WOLF

White Wolf is an end to end cyber security programme, designed for nation states with one clear objective: to protect and defend nation states from the threat of cyber damage.

White Wolf serves as a central location where a diverse set of capabilities and technologies come together to provide an ultimate cyber defence solution. Using the latest cyber defence technologies, processes, incident response, penetration testing, digital forensics and training, coupled with some of the best minds in the fields of defence, monitoring, central intelligence and cyber security, White Wolf is able to provide a holistic and unique service that allows leadership to fully address the growing problems of cyber crime affecting their nation.

As the nucleus to your nation's Cyber Security White Wolf enables your country to gear up against the threat of cyber by offering the following strengths:

Next Generation Security Operation Center SOC
A command and control unit, SOCs are the focal point for safeguarding against cyber related incidents, monitoring security, and protecting assets of the government network and endpoints. White Wolf SOCs provide situational awareness and continuous surveillance, including monitoring traffic, blocking unwanted traffic to and from the Internet, and detecting any type of attack.

CERT - Incident Response
Computer emergency response team, White Wolf - CERT strives for a safer, stronger Internet for all nation citizens by responding to major incidents, analyzing threats, and exchanging critical cyber security information with trusted partners around the world.

Forensics
Governments need skilled personnel to perform media exploitation and recover key intelligence available on adversary systems. To help solve these challenges, we provide digital forensic professionals and cyber crime law enforcement agents to piece together a comprehensive account of what happened.

Red and Blue Teaming
Because offense must inform defense, our experts provide enormous value to a government by applying social and technical attack techniques to find security vulnerabilities, analyze their risk implications, write modern exploits, and recommend mitigations before those vulnerabilities are exploited by real world attackers.

Training
We have created a leading-edge centre for bespoke cyber learning that your analysts and engineers can learn from. We offer a blended framework of e-learning, virtual classrooms and workshop-based face-to-face training. We categorize our training into general security awareness programmes, technical training and advanced cyber training.

Strategy & Consulting
The White Wolf centre is the nucleus to your country's security. Our subject matter experts will work hand in hand with you to advise on how best to design, implement and execute your security strategies, or to address your security concerns, whether these are strategies and security programmes for the whole nation or more specific to a certain industry or government agency.

1. COMMAND & CONTROL

Effective command and control is facilitated by being able to see everything that's happening on the Internet that affects your Nation and identifying and responding to potential threats. Internet activity will include activity initiated within your borders, activity targeting systems in your network and Internet traffic that is transiently routed through your networks destined for third countries. The White Wolf security operations centre (SOC) provides all the data, indexing, anomaly detections and reporting needed to build your command and control capability. White Wolf enables you to implement policies to protect your Nation and monitor for non-compliant activity.

Access to indexed data gives you full visibility of the content of Internet activity showing what systems are active and their behaviour and which applications are being used. The White Wolf SOC uses deep learning to assist in the detection of new threats and suspicious activity.

The SOC has a playbook of typical responses to known threats which will include the integration of intelligence with actual network activity. With full visibility of Internet activity, you are able to respond to and investigate potential threats in real time giving you immediate feedback on the effectiveness of your responses. The SOC will coordinate responses within your country, liaising with infrastructure, service providers and government departments to minimise the impacts of cyber threats. The SOC will work with your country's Internet registries, Telecommunications Service Providers and other agencies to stop cyber attacks.

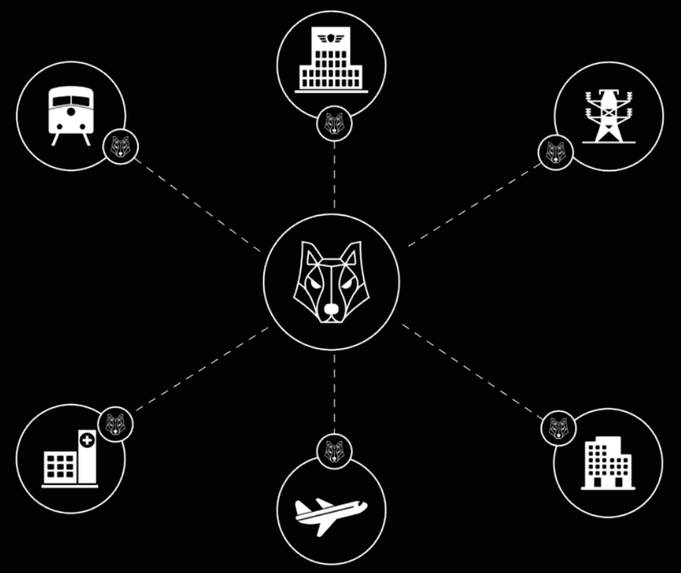
The state of the art White Wolf SOC gives you the information, technical knowledge and coordination capability to give you true command and control in your country's Internet infrastructures.

White Wolf Command and Control is architectured to be the central coordination point for all your critical national infrastructure units. It consists of a central Internet SOC and a number of local SOCs.

The Internet SOC provides analytics of the activities coming to or leaving the country to identify threats and early indicators of attacks. It allows nationwide responses against severe attacks where a critical response is required.

Local SOCs are deployed in the critical infrastructure that supports the nation, including transport, food, finance, government, telecommunications, health, power supply and any other service identified as critical for the nation. They are able to act locally, identifying threats that affect them and to take local actions to reduce the impact of an attack.

White Wolf Command and Control aggregates and analyses the intelligence collected by the Internet SOC and the local SOCs to early detect indicators of activities that put at risk the nation and that require an immediate and coordinated response. Crisis training, simulation and guidelines allow the teams to be ready to react effectively. As a result, attacks can be contained and their impact minimised. Additionally, the command and control preventive and investigation activities provide guidance and policies to coordinate protective measures and post-incident investigations that raise the overall protection for the critical national infrastructure.



NEXT GENERATION TECHNOLOGY

White Wolf SOCs are based around a security information and event management (SIEM) system which aggregates and correlates data from security feeds such as network discovery and vulnerability assessment systems; governance, risk and compliance (GRC) systems; web site assessment and monitoring systems, application and database scanners; intrusion detection systems (IDS); intrusion prevention system (IPS); log management systems; network behavior analysis and Cyber threat intelligence; wireless intrusion prevention system; firewalls, enterprise antivirus and unified threat management (UTM).

In addition to this, our SOCs use a revolutionary new layer of capability that enables investigators to see threats that were not visible until now - by leveraging our own patented technology, FT Government, analysts are able to detect and analyse threats in minutes and to neutralise them in seconds. Built by some of the best scientists in the United Kingdom, FT Government uses machine learning to revolutionize the way in which incidents are dealt with.

FT GOVERNMENT

The additional layer of defence found in our White Wolf SOCs uses our own technology, FT Government, which is built to meet the needs of even the most sophisticated networks. Everything from the detection of events through to the generation of reports has been developed by our engineers to ensure speed and scalability. Our Core engine has been implemented and tested on networks with one terabit per second links — processing the entire network traffic, with zero packet loss, all in real time. Our solution is linearly scalable; we maintain our high performance on networks of any size or complexity.

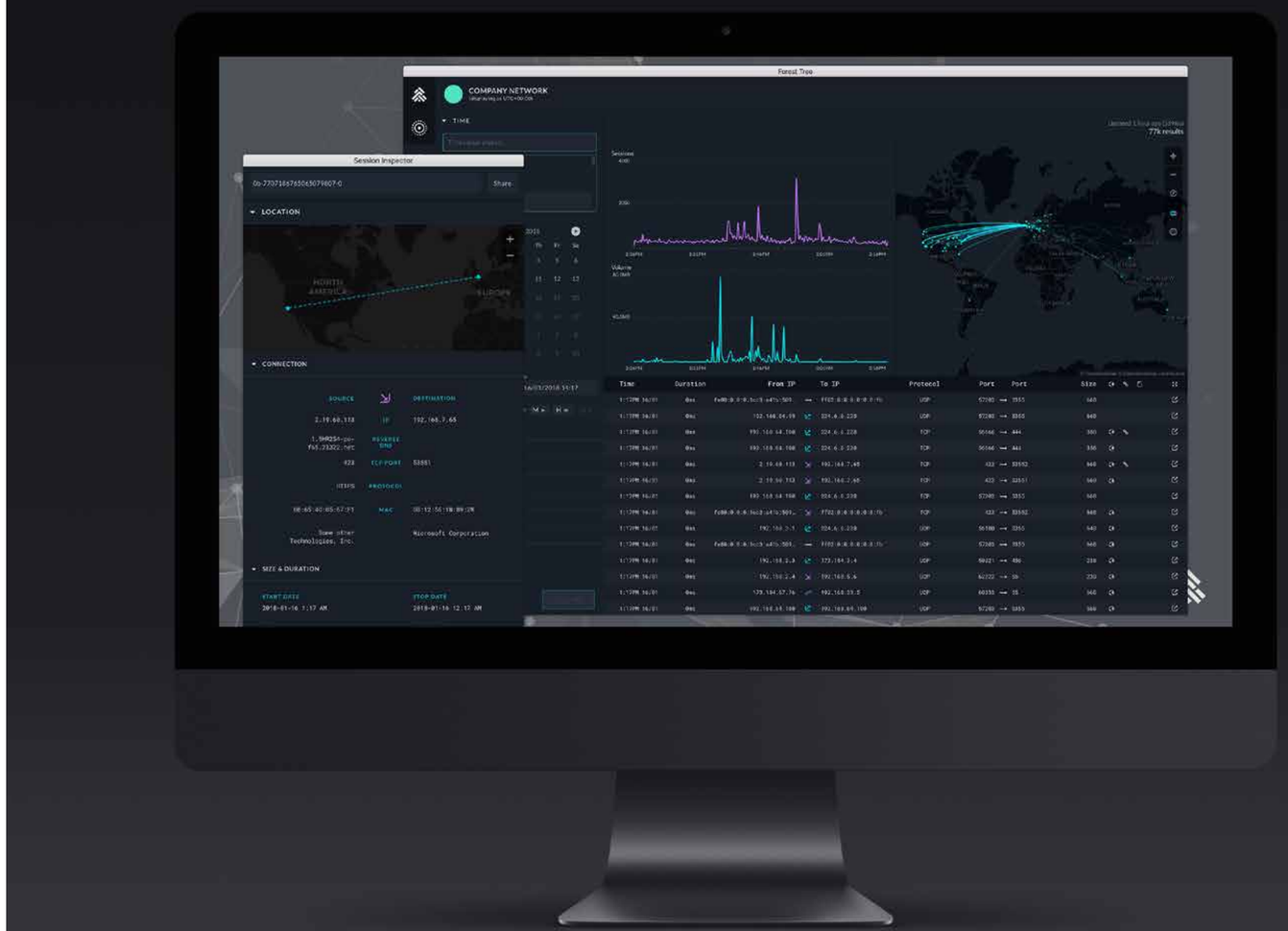
Delivers certainty.
Business decisions require accuracy. Our entire product has been developed and tested to ensure that you know exactly what actions are happening within your network at a given point in time. Its ability to act as a “black box” on the network, recording network activity for later investigation, gives certainty to your forensic investigations and incident reports. We help ensure your leadership are informed on any and all incidents before anyone else knows.

Built for quick results
Every part of our solution has been designed in consultation with security and governmental experts to ensure that it is as efficient and as effective as possible. The user experience has been carefully considered to ensure that analysts can get to the features they need quickly and the dashboards have been designed to ensure that each analyst is presented with the data they need to be able to perform their job. We work continuously with industry and governmental professionals to ensure our product meets the operational needs of security teams.

Designed for display.
We have carefully crafted dashboards and report templates that your leadership will want to see. Our clear graphical representations help articulate the complexities of your network traffic and risk in an inviting and engaging way.

Implement with ease.
The deployment of FT Government is highly simplified thanks to its flexibility and scalability. Once the connection points are identified, the traffic is sent to the platform for analysis. The process is the same regardless of whether the analysed flows are at national or organisational level.

As the platform works parallel to the network, there is no impact on the original traffic also running unnoticed to reduce its exposure to external threats.



2. CERT INCIDENT RESPONSE

At White Wolf, our CERT's function is to provide a centralised incident management response capability in the wake of major cyber attacks. It provides situational awareness, analysis of threats, and a main point of contact for international CERT engagement

The main benefits are:

- Develop an infrastructure for coordinating response to computer security incidents within a country or economy, e.g., for incident and threat activity related to any potential national risk(s) to its critical infrastructures, and on any perceived trends regarding future attacks and their precursors;

- Develop a capability to support incident reporting across a broad spectrum of sectors within a nation's borders;

- Conduct incident, vulnerability, and artifact analysis and to disseminate information about reported vulnerabilities and corresponding response strategies and to share knowledge and relevant mitigation strategies with appropriate constituents, partners, stakeholders and other trusted collaborators;

- Participate in cyber "watch" functions; encourage and promote a community of national and regional teams that share data, research, response strategies, and early warning notifications with each other and with similar points of contact throughout their own critical infrastructures and more broadly beyond their national borders;

- Help organizations and institutions within the nation develop their own incident management capabilities (e.g., provide guidance and information for planning and implementing the teams, build relationships and stimulate discussions among and across these government agencies, public/ private businesses, or academic organizations). This may also lead to developing baselines and benchmarking methods or evaluating the capabilities of these teams. This might also include a mechanism for certifying or accrediting CSIRT organizations with their country or economy.

3. FORENSICS

No one wants to think that a security breach will happen. But the reality is that the volume and variety of security attacks is rising. And today's attackers are clever and patient, often leaving almost no evidence that they were even there. Although it's important to take steps to prevent intrusions, if the unthinkable does happen, it's vital to quickly find out how the event occurred, minimize its impact, and do everything you can to prevent another breach. To investigate the incident, you must search for clues to quickly get the critical, in-depth information you need to find out exactly what really happened.

White Wolf Forensics, is a solution that can help you retrace the step-by-step occurrences of a security incident. It can help you to search, verify that an incident occurred, determine the severity, reconstruct the event, review it, determine the root cause, and take corrective and preventative action. Additionally, White Wolf Forensics can help show you the full extent of a breach via our FT Government technology data pivoting and comprehensive indexing capabilities.

White Wolf Incident Forensics:

- Retraces the step-by-step actions of cyber criminals to provide deep insights into the impact of intrusions and help prevent their reoccurrence.

- Reconstructs raw network data related to a security incident back into its original form for a greater understanding of the event.

Our diverse teams bring specialised technical and business knowledge. We have witnesses that have testified in court, arbitration, regulatory, and other proceedings globally. Our experienced teams of specialists have extensive technical and investigative knowledge and we have a global network of computer forensic examiners in various countries to assist with investigations. We bring value to our clients across numerous technical areas including cyber incident response, mobile device discovery and examinations, expert witness services and forensic investigations. We leverage in-depth knowledge of industry sectors based on years of experience working closely with our clients to provide you with a world class service

4. RED AND BLUE TEAMING

We use red and blue teaming and vulnerability assessments on your systems assess the security of your systems and people and to test the way in which they react to events. Vulnerability assessments help you find potential weaknesses in your service. Penetration tests proactively attack your systems to find weaknesses and help you understand how easy they are to exploit. Red teaming also includes the use of social engineering techniques that the criminals really use to be able to accurately assess how well prepared you are to deal with an attack.

When we're testing for vulnerabilities, our testing scope is wide enough to include the whole system and not just the software involved. For example, a wide testing scope could include:

- the security of the place where you keep equipment
- the interaction between an online system and a contact centre
- the people and their susceptibility to social engineering attacks

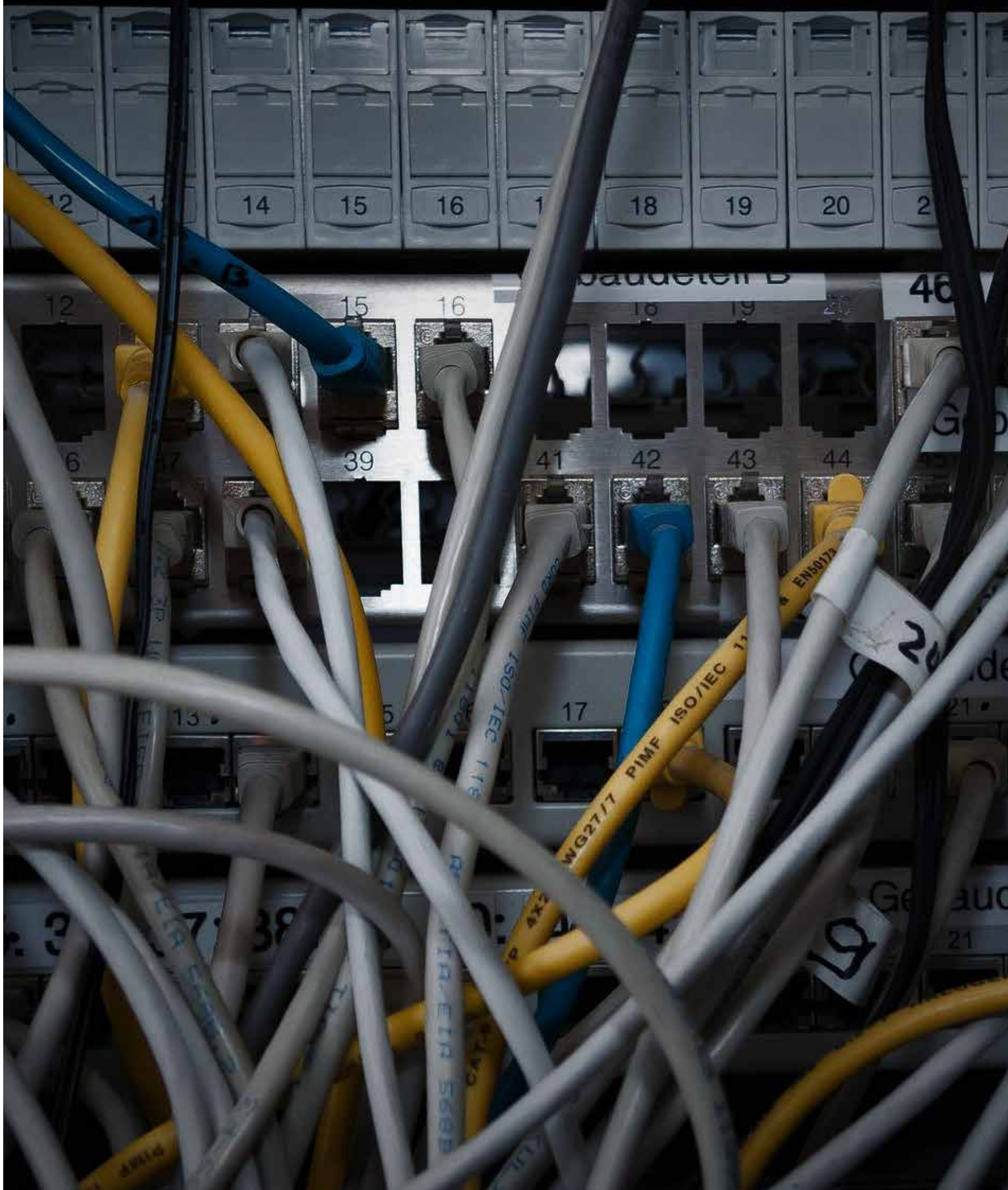
It's important for this service to make sure that people can't use offline information to exploit an online system. An example of this might involve getting a contact centre team to change a user's email address, then using a forgotten password function to access that person's account.

We will regularly assess your service's security, especially during major changes to your codebase (for example, when introducing a new dependency or integration).

When we perform the vulnerability assessment and penetration tests we will produce a report after every round of tests to explain what we did and what we found. This will be shared with your technical team, service manager and any senior managers that need to understand risks to your service.

The report summary will explain the risks in language that a non-technical audience can understand. The rest of the report will contain enough detail that your technical team can review and prioritise actions to fix any issues that have been found.

Unlike other penetration testing services who focus on assembly line assessments, we take a different approach. At Secgate, we deliver a quality product tailored to your needs. We work with our clients to build an accurate profile of what your primary function is, where threats come from, and what the goal of your security assessment is. This is done to ensure that the work conducted meets your exact needs and not just easily productized. We focus on long term relationships with our clients to ensure they get the best penetration test possible, offering them high-end, professional security audit services tailored to their needs.



5. TRAINING

We offer training through several delivery methods - live & virtual, classroom-style, online at your own pace or webcast with live instruction, guided study with a local mentor, or privately at your workplace. Our computer security courses are developed by industry leaders in numerous fields including cyber security training, network security, forensics, audit, security leadership, and application security. Courses are taught by real-world practitioners who are the best at ensuring you not only learn the material, but that you can apply it immediately when you return to the office.

Security Essentials Bootcamp Style
Hacker Techniques, Exploits & Incident Handling
Network Penetration Testing and Ethical Hacking
Web App Penetration Testing and Ethical Hacking
Intrusion Detection In-Depth
Advanced Penetration Testing, Exploit Writing, and Ethical Hacking
Securing Windows with the Critical Security Controls
Virtualization and Private Cloud Security
Advanced Security Essentials - Enterprise Defender
Implementing and Auditing the Critical Security Controls - In-Depth
Mobile Device Security and Ethical Hacking
Intro to Information Security
Perimeter Protection In-Depth
Securing Linux/Unix
Continuous Monitoring and Security Operations
Windows Forensic Analysis
Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Advanced Digital Forensics and Incident Response
Memory Forensics In-Depth
Mac Forensic Analysis
Advanced Network Forensics and Analysis
Advanced Smartphone Forensics

6. STRATEGIC ADVISORY

Cyber security has become a mandatory point in the agenda of every country. Major cyber attacks have been able to disrupt critical national infrastructures such as air transport or power supply. In some cases, they have even been used before a physical attack to highly reduce the response capabilities of a country.

Stability and control in the government of a country and the reputation abroad are the basis for an externally reliable country, and both can be impacted by weak cyber security. Alongside the direct financial threat of a major cyber attack, the damage to the reputation will harm inward investment into the country.

Secgate has a wealth of expertise in the definition and implementation of cyber security strategies at national level. By defining a long term strategy and supporting it with the appropriate regulations, an achievable baseline will be set that will increase the cyber security profile of the critical systems that support the nation. This approach can be extended to organisations working in specific sectors to ensure a consistent and effective protection.

Prevention is one of the aspects of cyber security, but reaction is equally important, especially at national level where coordinated and fast response is critical to contain the impact of an attack. Cyber Emergency Response Centres enable the coordination of activities and management of crisis effectively and efficiently. Secgate has experience in the definition and implementation of such centres, which need to be structured to cover the specific demands of different activity sectors.

The execution of the strategy and the associated operations need to be supported by professionals with the appropriate skillsets. The shortage of skilled cyber security professionals is a risk to any programme that can only be solved by putting in place an abilitation programme to sustain the strategy. Secgate has defined and executed cyber security enabling programmes at national level to ensure the professionals executing, maintaining and operating the cyber security strategy have the appropriate skillset and training for those tasks.


info@secgate.com
secgate.com
160 Fleet Street, London EC4A 2DQ