Forcepoint

Panic Stations

Overcoming the pressure to secure a high-threat, high-complexity cyber landscape

Foreword

"Across the globe, digital transformation continues to accelerate. Critical National Infrastructure (CNI) is no exception to this rule. The pursuit of Industry 4.0 in the heavy industries – spurring on the mass adoption of emerging technologies, like automation, 5G and the Industrial Internet of Things (IIoT) – as well as the drive towards greater connectedness in lighter industries, like the financial sector with Open Banking, is changing IT and OT (operational technology) environments.

"Alongside the advantages brought about by the transformation of CNI – including improved efficiency, productivity and sustainability – the rapid onset of new technologies has also introduced new risks. Greater interconnectedness and a higher volume of devices demand new approaches to security. Traditional methods for air gapping between IT and OT networks, for instance, cannot be applied to new concepts, like smart energy grids.

"The risk is heightened still by the fierce cyber threat landscape, with recent attacks on CNI demonstrating their attractiveness as a target due to their potential for spreading widespread disruption.

Take, for example, the 2021 attack on the Colonial Pipeline which halted operations of its 5,500 miles of pipeline on the East Coast and resulted in gas shortages. Or the ransomware attack on Travelex in 2020 that prevented the customers of many U.K. high-street banks from procuring foreign currencies.

"As our rapid digitization advances toward a new generation of CNI, we must endeavor to understand the impact of this tension between more advanced technologies and a heightened cyber landscape. Not only on our systems, but on those charged with securing this increasingly complicated environment. This will be essential to improving the resiliency of our CNI – a critical requirement for all of our safety and security."

Daniel Turner
Vice President | Forcepoint

The Threat Of Panic

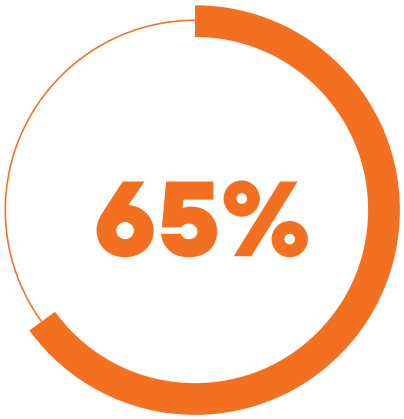
Recent high-profile cyberattacks have demonstrated the very real threat CNI providers face every day.

Our research of 500 U.S. and U.K. cybersecurity professionals working in CNI revealed that **65% of CNI organizations have fallen victim to a cyberattack in the past 12 months alone**. Some sectors have been hit worse than others: the rate of attack increases to three-quarters of organizations operating in the communications (75%), energy (74%) and banking (74%) sectors, as well as in central government (75%).

Ransomware is perceived by cybersecurity professionals to present the greatest risk to CNI organizations. This is perhaps unsurprising given it is the preferred choice of both revered cybercrime gangs, like Twisted Spider and Lockbit Gang, as well as less sophisticated cybercriminals that prefer to 'spray-and-pray', indiscriminately sending out malicious content en masse in the hope that a number of users will engage with it.

In fact, **more than half (57%) of CNI organizations across both countries report having fallen victim to a ransomware attack in the past year, of whom 72% admitted to paying the ransom**.

This was the case for the world's largest beef producer, JBS USA, who released a statement in 2021 detailing that it had paid the equivalent of $11 million in ransom following a hack on its operations, with the CEO Andre Nogueira quoted as saying that "*[they] felt this decision had to be made to prevent any potential risk for [their] customers.*"[1]



of CNI organizations have **fallen victim to a cyberattack** in the past 12 months

of CNI that fell victim to ransomware attacks **paid the ransom**

The risk of widespread disruption to critical services will undoubtedly have influenced this high proportion of CNI organisations to pay the ransom. Particularly given how rational concern can quickly escalate into an irrational response in such circumstances. We saw this during the pandemic where fears over product shortages led to panic buying, such as of toilet roll. Or when concerns over petrol supplies in the U.K. in the summer of 2021 led to long queues outside gas stations.

Similarly, public panic in response to a cyberattack on our utilities or banking services could feasibly lead to more disruption and damage than the attack itself. And many **CNI organisations are understandably prepared to do whatever it takes to reduce that risk and that of the reputational damage that may ensue**.

Daniel Turner
Vice President | Forcepoint

The Threat Of Panic

The impact that cyberattacks on CNI could present to our everyday lives is a real concern to cybersecurity professionals.

When asked about different CNI attack scenarios, all respondents cited at least one which they believed would lead the general public to panic.

In the U.S., the greatest concern was of a power outage, which may have been influenced by the ransomware attack on the Colonial Pipeline in 2021.

The largest publicly disclosed cyberattack against U.S. CNI, the attack compromised multiple states of its IT systems. **In just two-hours, 100 gigabytes of data was stolen, before the attacks infected the network with ransomware.** To prevent the ransomware from spreading, the Colonial Pipeline was shut down and caused temporary fuel shortages across the East Coast, directly affecting 12,000 gas stations. Indeed, on May 14 it was reported that 87% of gas stations in Washington DC had gone dry.[2] The panic buying that ensued required to the Energy Secretary Jennifer Granholm to publicly state that "*there should be no cause for hoarding gasoline, especially in light of the fact that the pipeline should be substantially operational by the end of this week and over the weekend*".[3]

Cybersecurity professionals in the U.K. predicted that disruption to personal banking would cause the most panic. While across both regions, over two-fifths of cybersecurity professionals fear the general population would panic as a result of cyberattacks that take down telecoms services, the websites of government and public services, or which prevent public transport services from operating.

It is clear that cybersecurity professionals are aware of the risk that a successful attack on CNI poses – not only to their organization, but to those that use their critical services every day.

U.S. CNI cybersecurity professionals fear a **power outage** will cause the pubic to panic

U.K. CNI cybersecurity professionals predict **disruption to personal banking** will cause the pubic to panic

CNI has become a high value target to cybercriminals. Infiltrating a country's most essential services not only demonstrates their mature capabilities, but is a lucrative target as many organizations – often supported by the authorities – will do whatever it takes to prevent disruption to services.

Ransomware attacks now present a significant risk to healthcare providers due to the impact on their ability to provide core services. Indeed, an Alabama-based medical center now faces a lawsuit which alleges a cyberattack on the hospital resulted in an infant's death.

A number of cyberattacks on public transport in 2022 also resulted in significant disruption of services, including on the Italian State Railways and the Israeli Light Railway. Though the infiltration of a Florida water treatment plant in 2021 presented one of the greatest risks to human life. The malicious actor's attempt to increase the sodium hydroxide to dangerous levels could have poisoned the water supply.

Attacks that pose a high risk to CNI present a high reward to many cybercriminals. So it is unsurprising that cybercriminals pursue CNI at such a high rate and with increasingly innovative and sophisticated methods.

And the rate of attacks is made yet more concerning as cybercriminals look for to exploit the innovation and digitalization of CNI to create even greater disruption.

A Risky Climate

Cybersecurity professionals in CNI are now operating in an increasingly challenging cyber threat landscape due to the growing sophistication of threat actors, threat vectors, and the high-tech environments that they are charged with securing.

Threat Landscape

When asked about the threat actors that they believe pose the greatest risk to their organization, cybersecurity professionals believe that the motivations inspiring cyberattacks on CNI are:

1. **Cyber gangs demonstrating their capabilities.** Gangs originating from Russia, China, Iran and North Korea have all been reported in recent years to have targeted CNI. The attack on the Colonial Pipeline in 2021, for example, is understood to have been conducted by Russian cyber gang, Darkside.

2. **Acts of political retaliation.** The use of cyberattacks as a political tool has increased. Cyberattacks that originated from addresses in China and Russia were launched against Taiwan in August 2022, for example, as it welcomed U.S. House of Representatives Speaker Nancy Pelosi.[4]

3. **Acts of 'hacktivism'.** Hacktivist groups present a significant risk to CNI. The motivations can align with more traditional activism, such as the anti-nuclear movement, or as part of wider cyber trends. At the beginning of Russia's war on Ukraine, for example, the Vice Prime Minister of Ukraine and Minister of Digital Transformation of Ukraine, Mykhailo Fedorov, turned to Twitter to enlist hacktivists to support the country's "fight on the cyber front".[5]

4. **Acts of cyber warfare.** The cyberattacks on CNI committed as part of the Russian war on the Ukraine, including alleged cyberattacks on Ukraine's power grid, has led to many now referring to the war as the first cyberwar.

A Risky Climate

The threats that CNI organizations face are broad and range significantly. In healthcare, for example, "drive-by-download" attacks and phishing attacks were cited as posing amongst the greatest risk to their organization by 64% of respondents, compared with just 11% of those working in public services. While in energy, **the greatest threats are perceived to be ransomware**, Internet of Things (IoT)-based attacks, and DoS and DDoS attacks.

The diverse reporting on the attack vectors that pose the greatest risk highlights the broad threat landscape that organizations in CNI are facing, because while some attack vectors may be less common against certain sectors today, their use by threat actors against other CNI organizations shows that they could easily be redirected toward them in the future.

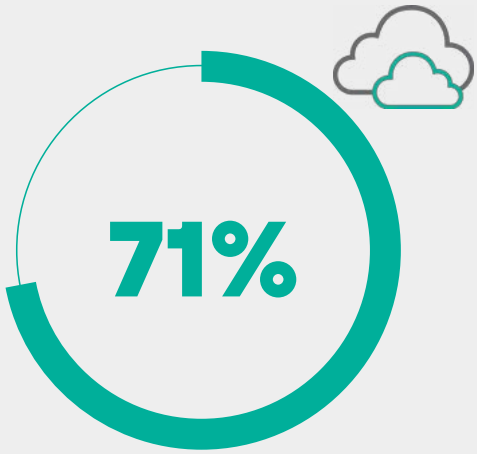
Ransomware, DoS and DDoS attacks
pose the greatest threat to the energy sector

Phishing and IoT-based attacks
pose the greatest threat to the banking sector

Rapid Transformation

The pursuit of digital transformation across the CNI sectors is also introducing new challenges for cybersecurity professionals due to the rapidly changing environment that they are required to secure.

Cloud migration is at the heart of many CNI organizations' digital transformation. Nearly one-fifth of CNI cybersecurity professionals report that their organization has already completed migration projects into public and private clouds (17% and 16%), while a further 49% and 48% report that such projects are underway or are planned within the next 12 months. However, the rate of adoption is faster in the U.K. than in the U.S. One-quarter of U.K. organizations (25%) have completed a public cloud migration compared with just 8% of US organizations.



71% of CNI organizations are working on or planning projects in the public or private cloud over the coming 24 months

The modernization of legacy systems and applications is also a priority amongst most U.S. and U.K. CNI organizations. **Nearly nine in 10 report that they have either completed these projects or will launch them within the next 24 months** (85% and 89% respectively). However, there is a disparity between industries. The communications sector is making the greatest investment in legacy system modernization with 38% of organizations across both regions citing having completed projects, compared with just 16% of those operating in banking, or food and agriculture.

Finally, the pursuit of new emerging technologies is widespread. **The use of Artificial Intelligence (AI) is becoming more prominent with nearly one in five organizations having completed projects for AI applications or AIOps** (AI for IT operations) (17% respectively), and nearly half of organizations again currently pursuing a project or planning on working on one over the next 12 months (48% and 49%). Similarly, 16% of organizations have completed projects for the IIoT, with a further 45% working on it currently or planning to in the next year. Though the rate of adoption is markedly higher in certain industries with one quarter of organizations in healthcare (27%), emergency services (26%) and critical manufacturing (24%) having already completed IIoT projects.

This rapid transformation of the IT and OT environments introduces new challenges to cybersecurity professionals in CNI. Indeed, when asked about the impact of the pursuit of digital transformation in their organization, the most commonly cited concerns were the need to secure new technologies both because they hadn't been used before, and due to them not having a strong security posture or being difficult to secure.

A similar number cited a shortage of security talent to secure this new digital infrastructure as a concern, which reflects the findings of CyberSeek, a project which is supported by the National Initiative for Cybersecurity Education (NICE), of the National Institute of Standards and Technology in the U.S. Department of Commerce. CyberSeek reports that between May 2021 and April 2022 there were over 700,000 cybersecurity job openings in the U.S., which is a staggering figure given that the total employed cybersecurity workforce totaled just over 1 million.[6]

Panic Stations

Overcoming the pressure to secure the world's most important infrastructure and institutions

The widespread disruption that cyberattacks on Critical National Infrastructure (CNI) can provoke has driven cybercriminals to target it with the full weight of their aggressions.

of CNI organizations have fallen victim to a cyberattack in the **past 12 months**

The threat of ransomware is of significant concern to CNI cybersecurity professionals

57% of CNI organizations fell victim to a **ransomware attack** in the past year...

...of whom 72% **paid the ransom**

Ransomware is perceived by cybersecurity professionals to be the **#1 cyber threat** to CNI

Securing CNI has become more challenging in recent years due to:

Digital Transformation

The pursuit of greater automation and interconnectedness, for example with the pursuit of Industry 4.0 and Open Banking, is making IT and OT environments more complex and requires cybersecurity professionals to secure new technologies they have little or no experience of.

Fierce cyber threat landscape

Cybersecurity professionals in CNI face a myriad of threats. Cybergangs demonstrating their capabilities and hacktivism are among their attackers' primary motivations. With political retaliation and cyber warfare also representing a significant threat in this tense geopolitical climate.

The potential consequences of a successful attack are high due to the risk of widespread disruption to core services. All cybersecurity professionals believe an attack on CNI could lead the public to panic.

US professionals believe an attack causing a **power outage** would cause the greatest panic

UK professionals believe an attack causing disruption to **personal banking services** would cause the greatest panic

The pressure to secure some of their nation's most important intrastructure and institutions is having an impact on the wellbeing of cybersecurity professionals working in CNI - over one third report that it is affecting their:

Performance & productivity at work

Personal & professional relationships

Personal wellbeing due to feelings of stress, anxiety and burnout

"As our rapid digitization advances toward a new generation of CNI, we must endeavor to understand the impact of this tension between more advanced technologies and a heightened cyber landscape. Not only on our systems, but on those charged with securing this increasingly complicated environment. This will be essential to improving the resiliency of our CNI - a critical requirement for all of our safety and security."

Daniel Turner | Vice President, Forcepoint

Now is not the time to panic

The heightened cyber threat landscape coupled with the rapid pursuit of digital transformation has created a high pressure environment for cybersecurity professionals working in CNI. Our research has unfortunately found that some professionals are starting to feel this pressure and it is having an impact on their professional and personal wellbeing. Feelings of stress, anxiety and burnout are affecting over one-third of all CNI cybersecurity professionals (35%, 39% and 36%).

Two-fifths of cybersecurity professionals report that the pressure to secure CNI has led them to have a low morale at work (40%), rising to 51% of U.K. employees. A similar number believe that it has in turn had a negative impact on both their performance and productivity at work, as well as on their professional relationships (37%, 38% and 38%). Once again, the rate for U.K. employees was higher with at least half reporting a negative impact on their performance, productivity and professional relationships in the workplace (52%, 50%, and 47%).

What is perhaps most concerning is the impact they report it is having on their personal wellbeing. Again, one-third report that the pressure has led them to start engaging in unhealthy behaviors, such as smoking or poor dietary patterns (35%), rising to 45% among CISOs. And 37% said that the pressure to secure CNI has negatively affected their personal relationships as well, once again rising to 50% among U.K. respondents.

These stark consequences on the professional and personal wellbeing of the cybersecurity professionals charged with securing CNI show that change is needed.

1/3

of CNI cybersecurity professionals are feeling **stressed and burnt out**

of CNI cybersecurity professionals are engaging in **unhealthy behaviors** due to the pressure

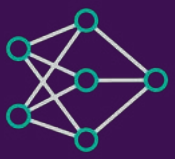
Trust Overcomes Fear

There is no compromise when it comes to securing CNI. The ferocity of the cyber threat landscape is unlikely to abate, and the pursuit of digital transformation is critical to driving efficiencies that will improve the productivity, sustainability and the profitability of CNI organizations.

The focus must therefore be on protecting the IT and OT environment that supports the personal resilience of the cybersecurity professionals that secure it. As identified earlier in this report, the focus must be on reducing the complexity for cybersecurity professionals and empowering them with the tools that will help them secure new technologies as they are introduced into the IT and OT environments alongside legacy applications and architectures.

What can organizations do to improve the resiliency of the high tech and high threat environment that they are now operating?

- **Make cyber hygiene the priority.** Make sure that you not only have set the right practices for ensuring the security of networks and the safe handling of data, but that they are maintained and updated as digitalization transforms IT and OT environments. Regular patching and back-ups with 3-disk redundancy are critical and can prevent most low-level attacks.



- **Simplify in the face of complexity.** As IT and operating environments have expanded and the threat landscape has become more complex, the number of tools cybersecurity professionals must manage has increased in turn. And each integration also increases the risk of a potential crack in the armor. **44% of cybersecurity professionals in CNI want to reduce the number of different tools they use to manage their organization's security environment** – rising to 50% of CISOs. Consolidated security platforms help reduce the number of tools needed to manage their security posture.

By 2025, 80% of enterprises will have adopted a strategy to unify web, cloud and private application access using a SASE/SSE architecture, up from 20% in 2021.[7]

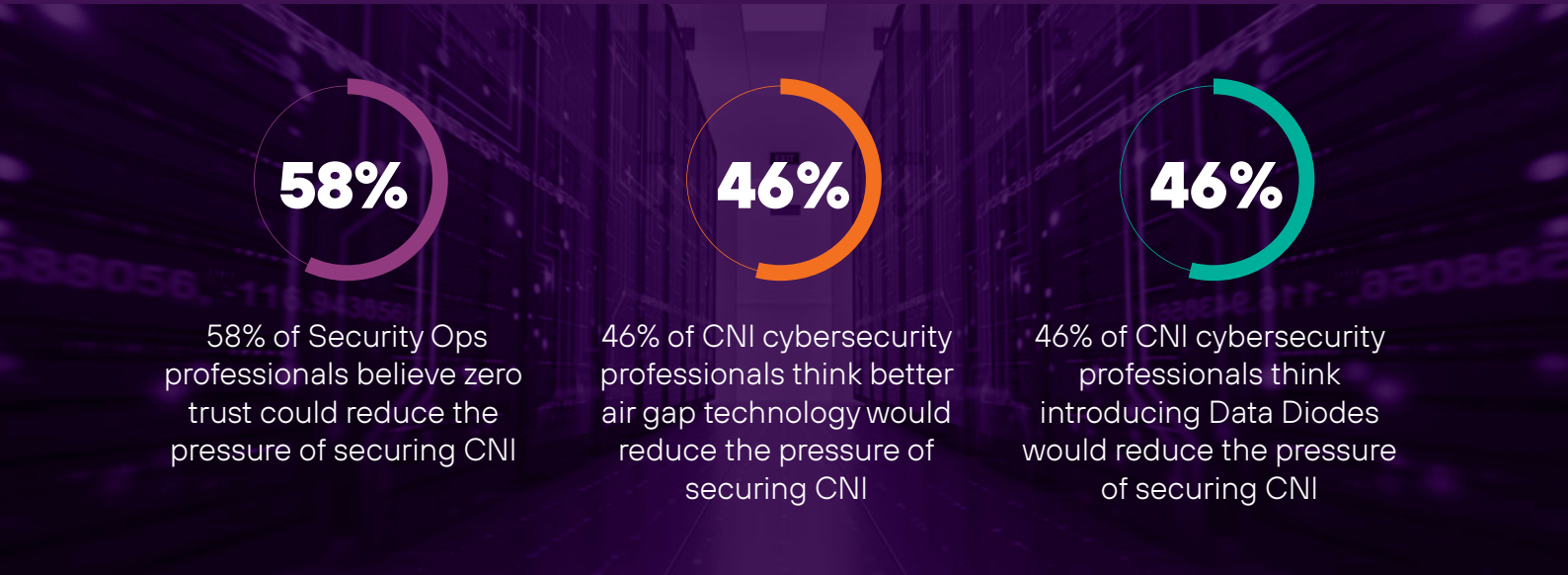
Gartner® 2022 Strategic Roadmap for SASE Convergence

Trust Overcomes Fear

- **Embrace Zero Trust.** Encouraging the entire organization to adopt a zero trust framework was called out by 43% of cybersecurity professionals as an approach that would help to reduce the pressure of securing CNI – rising to 58% among security operations professionals. The framework relies on the philosophy of **"never trust, always verify"** and encompasses a range of different technologies and best practices that center around reliably knowing who is trying to access or use data, and whether they have explicit permission to do so. This helps frustrate threats that have already infiltrated a network, as well as the explicit actions of employees acting maliciously.

- **Secure the route to the cloud.** With 71% currently working on or planning projects in the public cloud or private cloud over the coming 24 months, it is unsurprising that **46% of cybersecurity professionals in CNI would like to introduce better air gap security to secure the route to the cloud.** A zero-trust security posture for all inbound content arriving at the enterprise network - for instance, via email, web, file upload, removable drives, or social media – establishes a modern air gap between connected networks and services, as it mitigates the risk of embedded, concealed malware before it can enter the network. Adopting zero trust CDR services (Content Disarm and Reconstruction products) where no content crosses the network barrier, instead creating a clean replica of the content within the organization's IT environment, prevents known and zero day attacks found in file-based malware.

- **Implementing Secure Data Flows.** The increasing interconnectedness of IT and OT networks requires cybersecurity professionals to secure the flows of data between networks and devices. One approach is to create one-way data channels between trusted and untrusted networks, so data can be received but is never permitted to exit. Indeed, nearly half of cybersecurity professionals in CNI (46%) believe that the introduction of Data Diodes for a one-way data flow and physical network separation would help reduce the challenge of securing CNI. **An emerging class of diodes designed for two-way data flows can extend their usage into environments where bidirectional transfers of data are needed between IT and OT networks, such as OT monitoring in the cloud.**



58% of Security Ops professionals believe zero trust could reduce the pressure of securing CNI

46% of CNI cybersecurity professionals think better air gap technology would reduce the pressure of securing CNI

46% of CNI cybersecurity professionals think introducing Data Diodes would reduce the pressure of securing CNI

Cybersecurity professionals in CNI today face a climate characterized by high-risk, diverse threats, and where the rapid adoption of new technologies is revolutionizing both how organizations operate and what it takes to secure them.

The importance of their work cannot be underestimated. We all benefit every day from their efforts to ensure that no new threat or new technology puts our access to essential services at risk of disruption.

But now we understand the challenges they are facing, we have to find better solutions that will help alleviate the professional and personal burden that so many are carrying.

Making sure the transformation of security technologies and processes keeps pace with the ever-changing threat and IT landscapes, will be critical to ensuring a sustainable, secure and safe future for all.

Daniel Turner
Vice President | Forcepoint

Methodology

This report was conducted by Censuswide in July, 2022. It was commissioned by Forcepoint and surveyed 500 cybersecurity professionals working in Critical National Infrastructure (CNI), split equally across the UK and US. Censuswide abides by and employs members of the Market Research Society which is based on the ESOMAR principles, they are also members of the British Polling Council.

Gartner 2022 Strategic Roadmap for SASE Convergence, Neil MacDonald, Andrew Lerner, John Watts, 24 June 2022

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

References

[1] **JBS USA Cyberattack Media Statement** 09 June 2021, JBS Foods, accessed 08 August 2022 <https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9>

[2] **Cyberattacks on our energy infrastructure: The need for a national response to a national security threat** 13 December 2021, Atlantic Council, accessed 08 August 2022 <https://www.atlanticcouncil.org/blogs/energysource/cyberattacks-on-our-energy-infrastructure>

[3] **Press Briefing by Press Secretary Jen Psaki, Secretary of Energy Jennifer Granholm, and Secretary of Homeland Security Alejandro Mayorkas** 11 May 2021, The White House, accessed 08 August 2022 <https://www.whitehouse.gov/briefing-room/press-briefings/2021/05/11/press-briefing-by-press-secretary-jen-psaki-secretary-of-energy-jennifer-granholm-and-secretary-of-homeland-security-alejandro-mayorkas-may-11-2021/>

[4] **From 7-11s to train stations, cyber attacks plague Taiwan over Pelosi visit** 04 August 2021, Reuters, accessed 09 August 2022 <https://www.reuters.com/technology/7-11s-train-stations-cyber-attacks-plague-taiwan-over-pelosi-visit-2022-08-04/>

[5] **@FedorovMykhailo** 26 February 2022. "*We are creating an IT army. We need digital talents. All operational tasks will be given here: https://t.me/itarmyofurraine. There will be tasks for everyone. We continue to fight on the cyber front. The first task is on the channel for cyber specialists.*" [Twitter post] <https://twitter.com/FedorovMykhailo/status/1497642156076511233>

[6] **Cybersecurity Supply and Demand Heat Map** April 2022, CyberSeek, accessed 08 August 2022 <https://www.cyberseek.org/heatmap.html>

[7] **Gartner®: 2022 Strategic Roadmap for SASE Convergence, Neil MacDonald, Andrew Lerner** 24 June 2022 and ID G00770805


Forcepoint