ARMIS®

THE STATE OF CYBERWARFARE

ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

COUNTRY-BY-COUNTRY ANALYSIS

THE NETHERLANDS

TABLE OF CONTENTS

INTRODUCTION

If you've reviewed the global Armis State of Cyberwarfare and Trends Report: 2022-2023, you know that it's critical for business and IT leaders to understand the evolving threat landscape surrounding cyberwarfare, so that they can improve their cybersecurity posture to defend against these attacks. To prepare this report, Armis commissioned a study surveying 6,021 IT and security professionals globally to determine worldwide trends as they relate to security professionals' sentiments on cyberwarfare, attack patterns, cyber spending, and more. Responses were gathered between September 22, 2022 and October 5, 2022.

Armis utilized data from its award-winning Asset Intelligence and Security Platform to verify the survey results against real-world data trends. Proprietary data from the Armis platform collected June 1, 2022 through November 30, 2022 confirmed that cyberattacks haven't slowed, only worsened. Threat activity against the global Armis customer base increased by 15% from September to November when compared to the three months prior. Further, Armis identified the largest percentage of threat activity against critical infrastructure organizations, with healthcare organizations the second most targeted when compared to various industries.

In addition to these global findings, Armis has prepared regional findings and country-by-country analysis to offer unique, localized insights which may be more impactful for individual readers depending on where they physically are based and the counties in which their business operates. **For this country-by-country analysis, we will zoom in on the findings pulled from the 52 respondents who shared insights for our survey that are based out of the Netherlands and work across industries including healthcare, manufacturing, retail, financial services, and more.**

SUMMARY OF FINDINGS

Today's targets extend well beyond nation-states and affect any organization. Dutch scientists have warned organisations since the start of the war about cyberattacks affecting the critical infrastructure of other countries, for example, attacks on Ukraine's power grid could lead to blackouts in the Netherlands. Experts have been trying to raise awareness for more investments in cybersecurity by the Dutch government and organisations. Luckily, the government announced again large investments in cybersecurity during Prinsjesdag this year for 2023 and the coming years. The government is working on a strengthened approach to protecting Dutch critical infrastructure, in line with the implementation of the European Networks Information Security Directive (NIS2 Directive).

Besides the legislation efforts, Dutch companies also need to improve their cybersecurity posture. Armis research shows that 65% of Dutch companies agree that the war in Ukraine has led to an increased threat of cyberwarfare. This is quite worrying, and awareness is needed to get Dutch companies prepared for cyberwarfare.

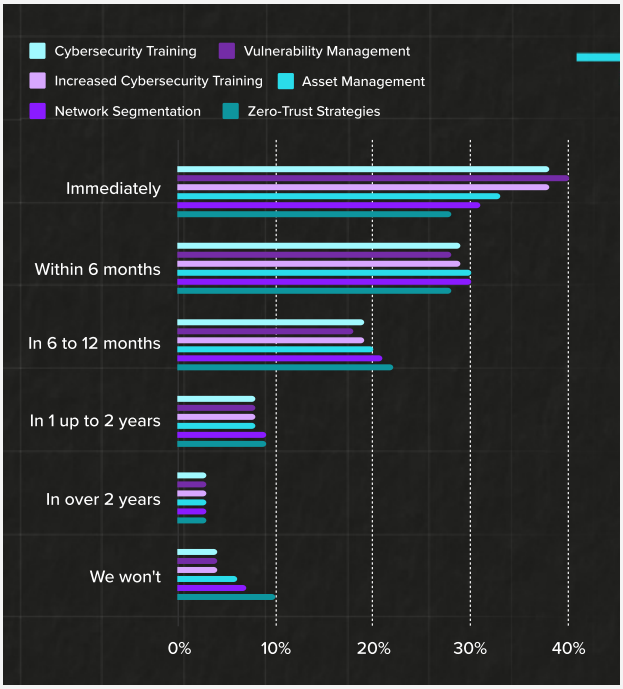
EMEA

Through the course of 2022, the EMEA region has been shocked by the invasion of the sovereign nation of Ukraine. With the geopolitical instability associated with physical warfare and cyberwarfare, shockwaves of consequences are arriving throughout the area. Unpredictability in the food supply, the infamous energy crisis, and a wave of cyberattacks focused against the most critical functions of society, are all contributing to changes in spending and priorities across numerous industries. The report confirms the rise in cyberattacks, bringing to light that almost 3 in 5 organisations (58%) experienced one or more cybersecurity breaches. And 25% of respondents confirmed that there has been an escalation in the number of threats to their organisation.

Measures are being taken to ensure protection, but to date, still less than half (44%) of IT and security professionals agree that their organisation has programs and practices in place to respond to cyberwarfare threats. Respondents depicted their company as ill-prepared as there are some relevant issues to be addressed:

- Only 46% of IT and security professionals in EMEA strongly agreed on knowing who to contact if they notice suspicious activity.
- Only 76% of IT and security professionals in EMEA said they collaborate with others in the industry when it comes to sharing information about threats, below the U.S. and APJ averages. Although being a high number, this indicates that there is still work to be done if all areas are to be shielded from cyberattacks.
- Only 33% of IT and security professionals in EMEA have reported an act of cyberwarfare to the authorities, below the US (63%) and APJ (61%) levels.
- Almost 2 in 10 (18%) of IT and security professionals in EMEA said their organisation does not have a contingency plan in place if cyberwarfare is detected.
- Only a third (33%) of IT and security professionals have a validated cyberwarfare plan with best practice frameworks, to be appropriate and proportionate.
- Moreover, less than half (49%) of companies are educating employees as a common practice, or restricting network admin rights (40%). Fewer still have cybersecurity practices implemented such as creating a security-focused work culture (37%), investing in cybersecurity insurance (31%), and implementing a Cyber Risk Framework (31%).

There is a disconnect between confidence levels of preparedness for cybersecurity attacks (84%) and reality, and investment is needed to close that gap, both for tools and services. When asked to select when they will invest in certain aspects, the following responses were given by IT professionals:



REGULATION IS PUSHING TOWARDS THE FUTURE

Governments, security services and related competent authorities continue to put great emphasis on the need for an improved cybersecurity posture, and the imperative necessity for a more cyber resilient strategy. The recent EU Cyber Resilience Act builds on the EU's existing Cybersecurity Directive of 2016, thus updating the bloc's requirements for enhanced cybersecurity by member states. Prior to this EU Cyber Resilience Act, much of the pressure when it came to cybersecurity was put on users of these products, both enterprises and individuals alike. Now, the manufacturer will share a larger part of this responsibility as well. Accountability can go a long way in helping to make improvements across the board. The EU also released NIS2, adding many more verticals into the spotlight and introducing fines, sanctions, and penalties, for not doing proper risk management, basic cyber hygiene, and taking undue delays in corrective action.

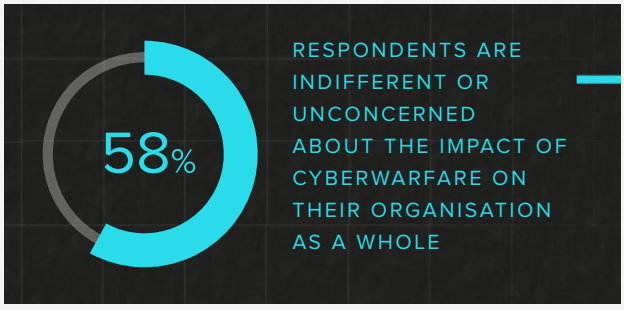
The emergence of regulations is a great conversation starter and will certainly help address that gap of investment in certain tools and prioritise their importance, but there is still a long way to go to secure the critical vulnerability gaps introduced by the exponential proliferation of connected assets. 37% of respondents agree that connected devices are a top priority in the event of a cyberwarfare attack.

Beyond the internal efforts, it is believed amongst IT professionals that the European Union and its member states should also boost cooperation with other allies around the world. More than half (61%) stated that they would support conscription into a cyber defence league if their country were drawn into a cyberwar conflict.

DUTCH TRENDS FROM THE ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

DUTCH COMPANIES NEED TO BE BETTER PREPARED FOR THREATS OF CYBERWARFARE

58% of Dutch companies are still not serious about the threat of cyberwarfare. These organisations say they are indifferent or unconcerned about the impact of cyberwarfare on their organisation as a whole. Compared to companies worldwide (average 24%), Dutch companies may be more aware of the dangers of cyberwarfare. To go further, 40% of Dutch IT professionals also say they are not prepared for cyberwarfare – a quite matching result and a worrying fact considering these are companies (with a likely low level of cybersecurity) that need to prevent an attack from another nation-state.



To zoom into the above results, the following findings on how Dutch companies prepare themselves for a cyberwarfare attack were found.

- Only 33% of Dutch IT professionals consider their organisation to be fully prepared to handle cyberwarfare. They have a plan that is validated with best practice frameworks, to be appropriate and proportionate.
- When looking into which cybersecurity practices are implemented in Dutch companies, 67% use anti-malware and firewall software, 60% back up data, and 54% encrypt data. However, only 29% create a security-focused work culture, 29% invest in cybersecurity insurance, and 31% are implementing a CRF Cyber Risk Framework.
- Of the respondents at Dutch companies, 75% say that the employees do get regular training on how to behave safely online.
- Luckily, Dutch companies do also invest in cybersecurity practices in the short term. Within six months, the top three investments are Network Segmentation (60%), Vulnerability Management (59%), and increasing cybersecurity training (52%).

THE WAR IN UKRAINE IS A WAKE-UP CALL FOR DUTCH COMPANIES

Dutch companies worry in terms of cybersecurity due to the war. 65% of Dutch companies agree that the war in Ukraine has led to an increased threat of cyberwarfare. More than half (63%) say they experienced more threat activity on their network between April and October 2022 compared to the previous six months. Enough reasons for the Dutch to invest in cybersecurity. As mentioned before, 58% of Dutch companies are still not serious about the threat of cyberwarfare. Looking at cybersecurity investments since the start of the war, 15% of Dutch companies have yet to increase investment in tools or services. However, there is increased investment in Vulnerability Management (38%) and Access Management (31%), which are still

quite low compared with EMEA. Nonetheless, Dutch companies have invested more than most EMEA countries in Identity Governance and Administration (42% over 29%). When looking ahead, 79% of IT professionals in the Netherlands think it's likely that their company invests more of its budget into cybersecurity due to such global events.

DUTCH COMPANIES TRUST IN THE GOVERNMENT'S ABILITIES TO DEFEND AGAINST CYBERWARFARE

The report also shows that Dutch companies are more confident that the government can and will defend them against cyberwarfare with 71% answering that they trust the government's abilities compared to an EMEA average of 66%. In the Netherlands, an increased political interest in securing digital infrastructure against state-sponsored threat actors and hacker groups has risen. The Dutch government announced again large investments in cybersecurity this year for 2023 and the coming years. The government is working on a strengthened approach to protecting Dutch critical infrastructure, in line with the implementation of the European Networks Information Security Directive (NIS2 Directive).

However, there is still some work to do by the government to gain more trust in the ability of public administrations to cope with a cyberwarfare attack. 44% of respondents think that public administrations are unable to cope. On the other side, Dutch companies are much more willing to collaborate with their industry when it comes to sharing information about threats (77%). Also, Dutch companies are willing to support conscription into a cyber defense league if their country was drawn into a cyber war conflict (60%).

WHY DO THESE FINDINGS MATTER?

The findings show that cyberattacks are influencing many business areas and that companies are prioritizing very differently in their cybersecurity efforts regionally – some more or less surprising.

> *"Due to global events such as the war in Ukraine, awareness for more cybersecurity investment and preparations is more needed than ever. Especially since threats of cyberwarfare are around the corner. Dutch companies definitely feel the need to take action and are – compared to other European countries – on the right path. However, their attitude towards this type of terrorism needs a lift as well."*
>
> **MIRKO BÜLLES**
> DIRECTOR OF TECHNICAL ACCOUNT MANAGEMENT EMEA/APAC AT ARMIS

WHAT CAN YOUR ORGANIZATION DO TO PROTECT ITSELF?

So, what can organizations do? Early detection and continuous monitoring is the best way to improve your organization's security posture and remediate quickly. After all, if you don't know you have a problem, you can't fix it. Similarly, if you can't see an asset, you can't protect it. This is where Armis can assist.

ARMIS ASSET INTELLIGENCE PLATFORM

The **Armis Asset Intelligence Platform** provides unified asset visibility and security across all asset types, including information technology (IT), internet of things (IoT), operational technology (OT), internet of medical things (IoMT), cloud, and cellular-IoT — both managed and unmanaged. Delivered as an agentless software-as-a-service (SaaS) platform, Armis seamlessly integrates with existing IT and security stacks to quickly deliver the contextual intelligence needed for improving an organization's security posture, without disrupting current operations or workflows. Armis helps customers protect against unseen operational and cyber risks, increase efficiencies, optimize the use of resources, and safely innovate with new technologies to grow their business – no matter the threat, cyberwarfare or other.

Register today for a Security Risk Assessment to learn which assets are most vulnerable to attack. Use these insights to prioritize your risk mitigation strategy and ensure full compliance with regulatory frameworks that require you to identify and prioritize all vulnerabilities.

To request a custom demo from Armis, please visit: armis.com/demo.

To dive deeper into the findings of the Armis State of Cyberwarfare and Trends Report: 2022-2023 on a global scale, please visit: **armis.com/cyberwarfare.**

THE STATE OF
CYBERWARFARE

ABOUT ARMIS

Armis, the leading asset visibility and security company, provides the industry's first unified asset intelligence platform designed to address the new extended attack surface that connected assets create. Fortune 100 companies trust our real-time and continuous protection to see with full context all managed, unmanaged assets across IT, cloud, IoT devices, medical devices (IoMT), operational technology (OT), industrial control systems (ICS), and 5G. Armis provides passive cyber asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in California.

armis.com

info@armis.com

20230110-1

ARMIS®