

Cyber Solutions **by** Thales

2022-2023 :
A year of Cyber Conflict
in Ukraine

Summary of extensive analysis from
the Thales Cyber Threat Intelligence Team



THALES
Building a future we can all trust

A YEAR OF CYBER CONFLICT IN UKRAINE

The Russian-Ukrainian conflict has profoundly changed the cyber threat landscape. The graphs presented in the following pages show how the conflict has unfolded from a cyber perspective, but also illustrate trends that go beyond the borders of Ukraine and Russia.

PERMANENT CYBER-WAR OR HIGH-INTENSITY HYBRID CYBER-CONFLICT?

The question of whether Russia and Ukraine are engaged in a full-scale cyber-war has been asked many times, but the trends that are evidenced in the graphs suggest that the situation on the ground does not really constitute a permanent cyber-war – or at least not any more.

FROM CONCENTRATED DESTRUCTION CAMPAIGNS TO ALL-OUT DDOS

We prefer to refer to high-intensity hybrid cyber conflict. This notion obviously includes acts of cyberwarfare, as were seen at the start of the

conflict and even before the invasion began in February 2022. Destructive military software programmes were pre-positioned in Ukrainian systems by Russia (see Figure 2) in an attempt to carry out a cyberwar as a counterpart to a lightning war on the ground. These wiper programs are examined in detail in Chapter 4.

From a cyber perspective, the conflict has clearly moved on from those early days. Since the third quarter of 2022, the cyber conflict has largely involved harassment and cyber disruption operations by hacktivists who are aligned with, though not necessarily sponsored.

These operations account for 75% of the incidents recorded since the beginning of the conflict, and involve waves of DDoS attacks carried out by groups that for the most part were formed after the conflict began. Destructive cyber-military operations account for only 2% of the total number of incidents and are mainly targeted at Ukrainian public-sector organisations.

FIGURE 1: FOCUS ON DDOS ATTACKS BY COUNTRY

From the initial diversification of the typology of cyber attacks to the massive use of DDOSS at the turn of the third quarter of 2022

3/4 of attacks are DDOS, massively supplanting other types of attacks such as data theft, phishing or espionage used at the margin.

Ukraine	162	Estonia	33	Austria	4
Poland	110	Denmark	21	Spain	3
Latvia	74	United Kingdom	16	Kazakhstan	3
Russia	70	Japan	15	Canada	3
Sweden	60	Moldova	14	Belarus	3
United States	57	France	13	Switzerland	2
Germany	52	Italy	12	Belgium	2
Lithuania	45	Bulgaria	11	Netherlands	1
Czech Republic	37	Finland	8	Luxembourg	1
		Romania	6	Israel	1
		Norway	6	Croatia	1
		Slovakia	5	Colombia	1
		Greece	5	Armenia	1

BREAKDOWN OF INCIDENTS BY MODE OF ATTACK AND MOTIVATION THROUGHOUT THE CONFLICT (GLOBAL SCALE)

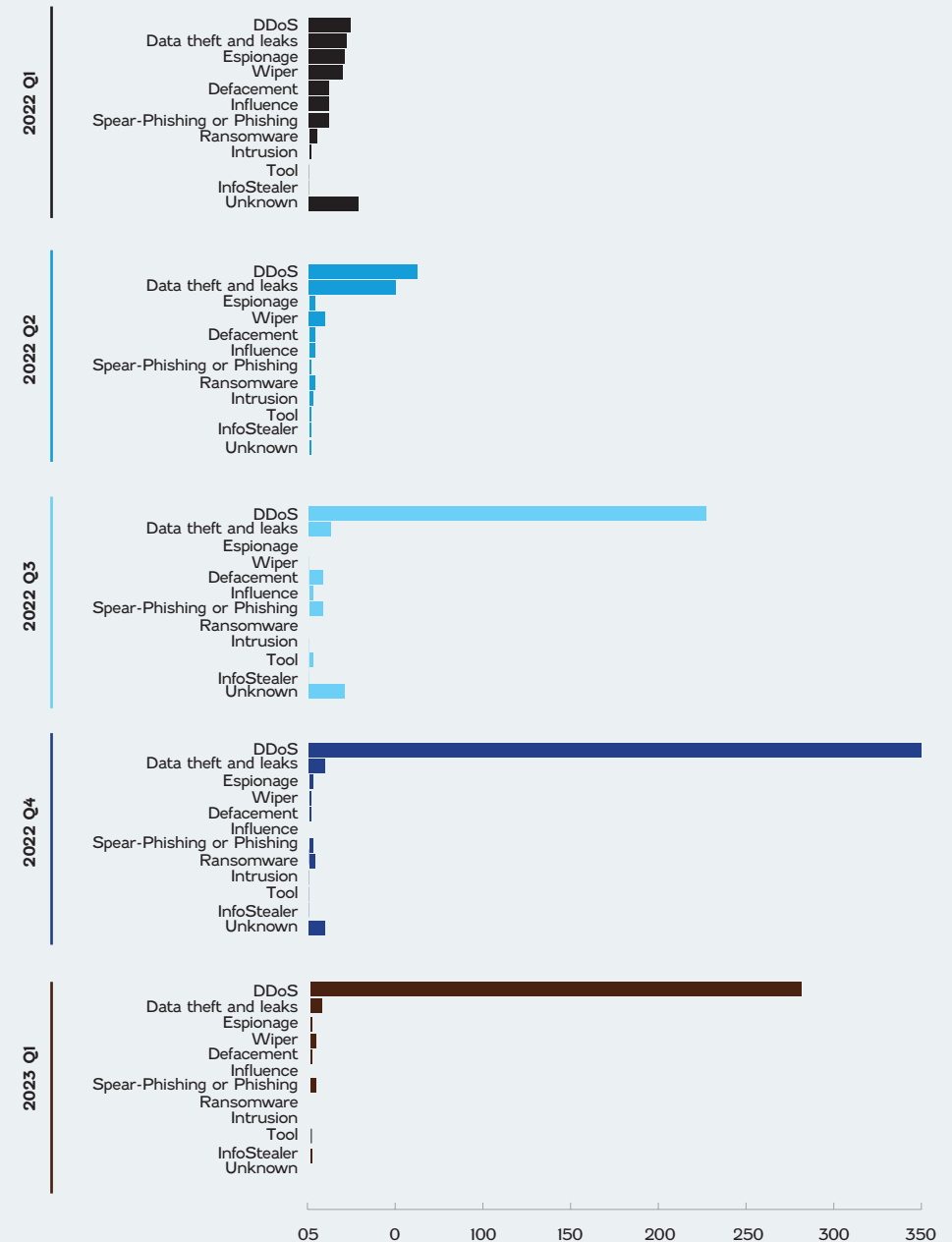
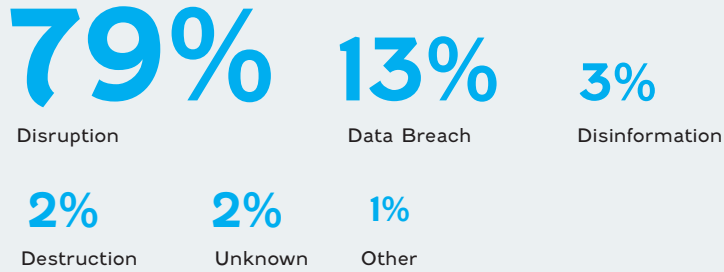
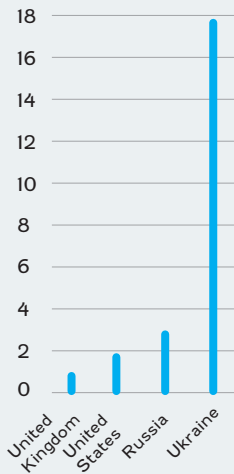


FIGURE 2:

_ATTACKERS' MOTIVATIONS



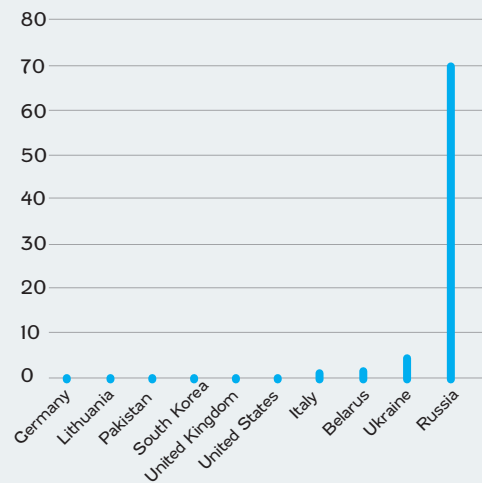
_ESPIONAGE BY COUNTRIES



_WIPER BY COUNTRY



_DATA THEFT AND LEAKS



_FROM THE FEAR OF APTS (ADVANCED PERSISTANT THREATS) TO THE AGE OF WAR HACKTIVISM

The overwhelming majority of the cyber actors involved in the conflict are unsponsored groups, and these groups have played a

role in the globalisation but also the hybridisation of the conflict. The KillNet galaxy, the Noname057 hacktivist network and the main pro-Russian hacktivist groups alone are responsible for more than 60% of incidents.

FIGURE 3: NUMBER OF ATTACKS PER ATTACKER GROUP (GLOBAL SCALE)
Pro-Russian hacktivists overrepresented among cyber attackers linked to Ukraine conflict



Demonstrating the existence of this phenomenon of hybrid cyber conflict, the number of incidents increased from an average of 1.6 incidents per day (45.9 per month)

between January and mid-July 2022 to 3.8 per day (117 per month) since then.

FIGURE 4: NUMBER OF INCIDENTS PER DAY SINCE THE BEGINNING OF THE CONFLICT (GLOBAL SCALE)

An acceleration in the number of attacks from the 2nd quarter of 2022

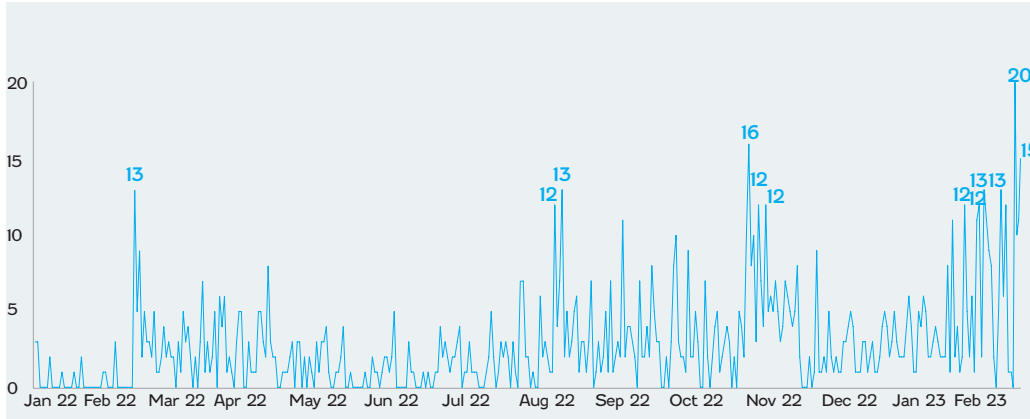
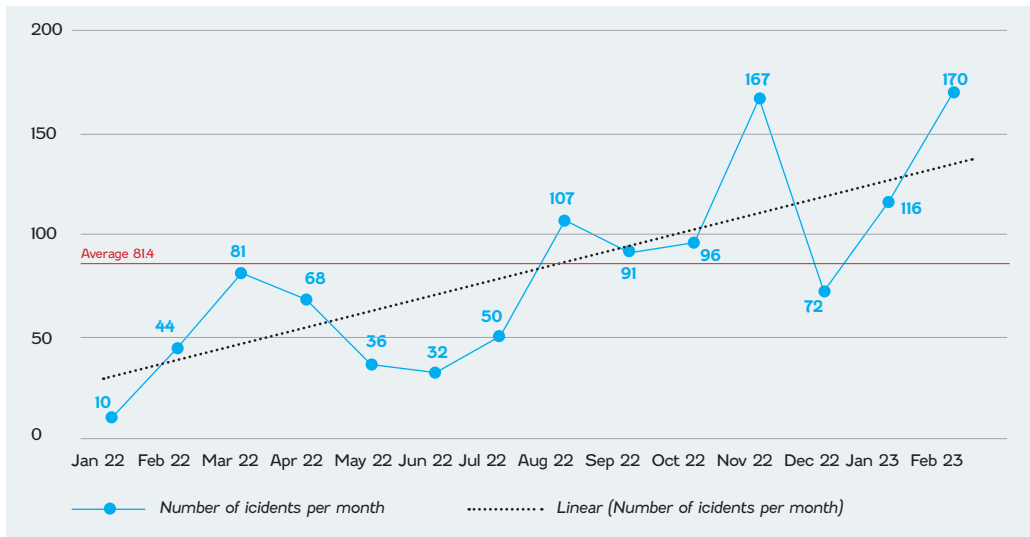


FIGURE 5: NUMBER OF INCIDENTS PER MONTH SINCE THE BEGINNING OF THE CONFLICT (GLOBAL SCALE)

An acceleration in the number of attacks from the 2nd quarter of 2022



Similarly, while most of the incidents carried out early in the conflict focused on the Ukrainian defence industrial base and the country's public administrations and government agencies, the focus has changed with the advent of war hacktivism.

_LATERALISATION OF THE CONFLICT IN EUROPE

The aviation sector, especially in the Nordic countries, the energy sector throughout Europe, the health sector, the banking and financial services sector, and also European public administrations, have witnessed a dramatic increase in the number of incidents.

FIGURE 6: BREAKDOWN OF INCIDENTS BY SECTOR OF ACTIVITY SINCE THE BEGINNING OF THE CONFLICT (GLOBAL SCALE)

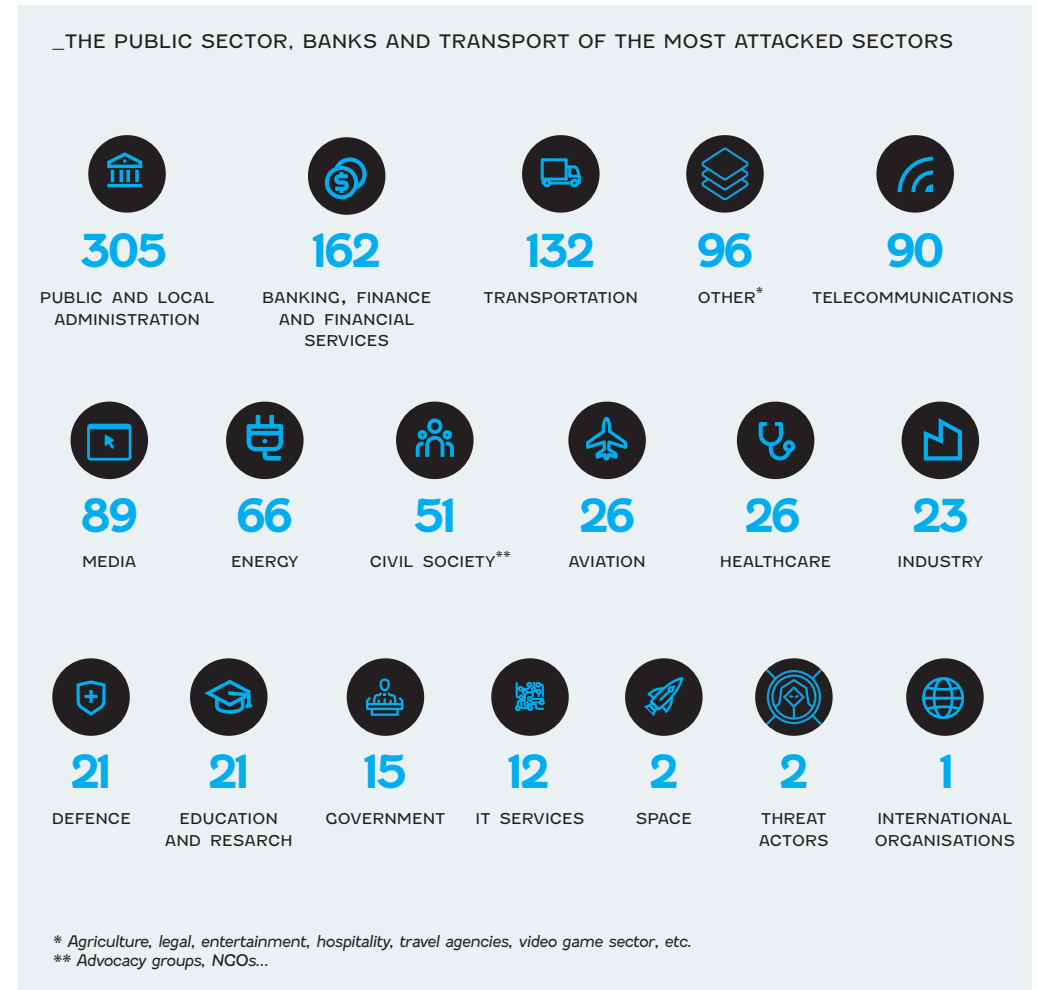
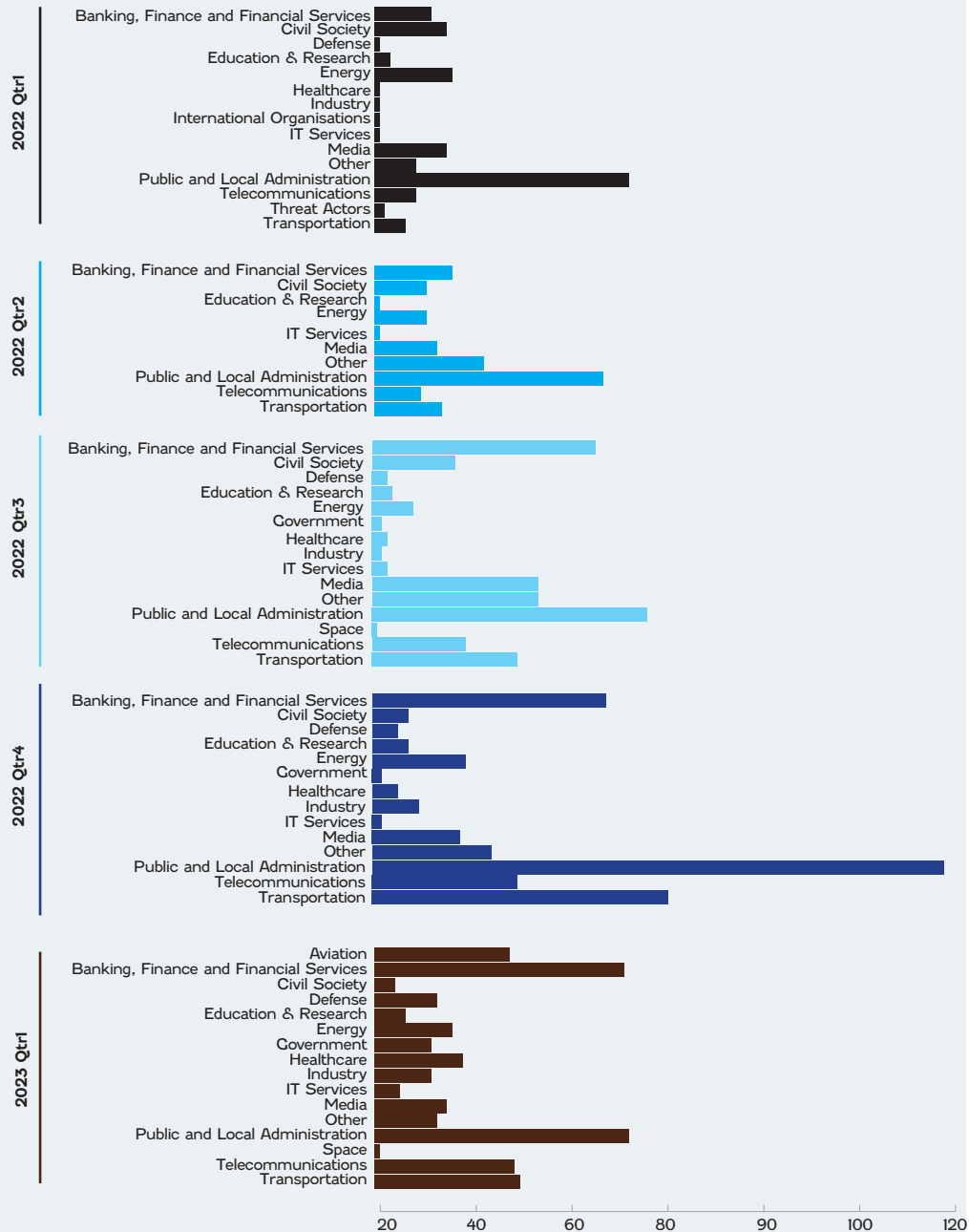


FIGURE 7:

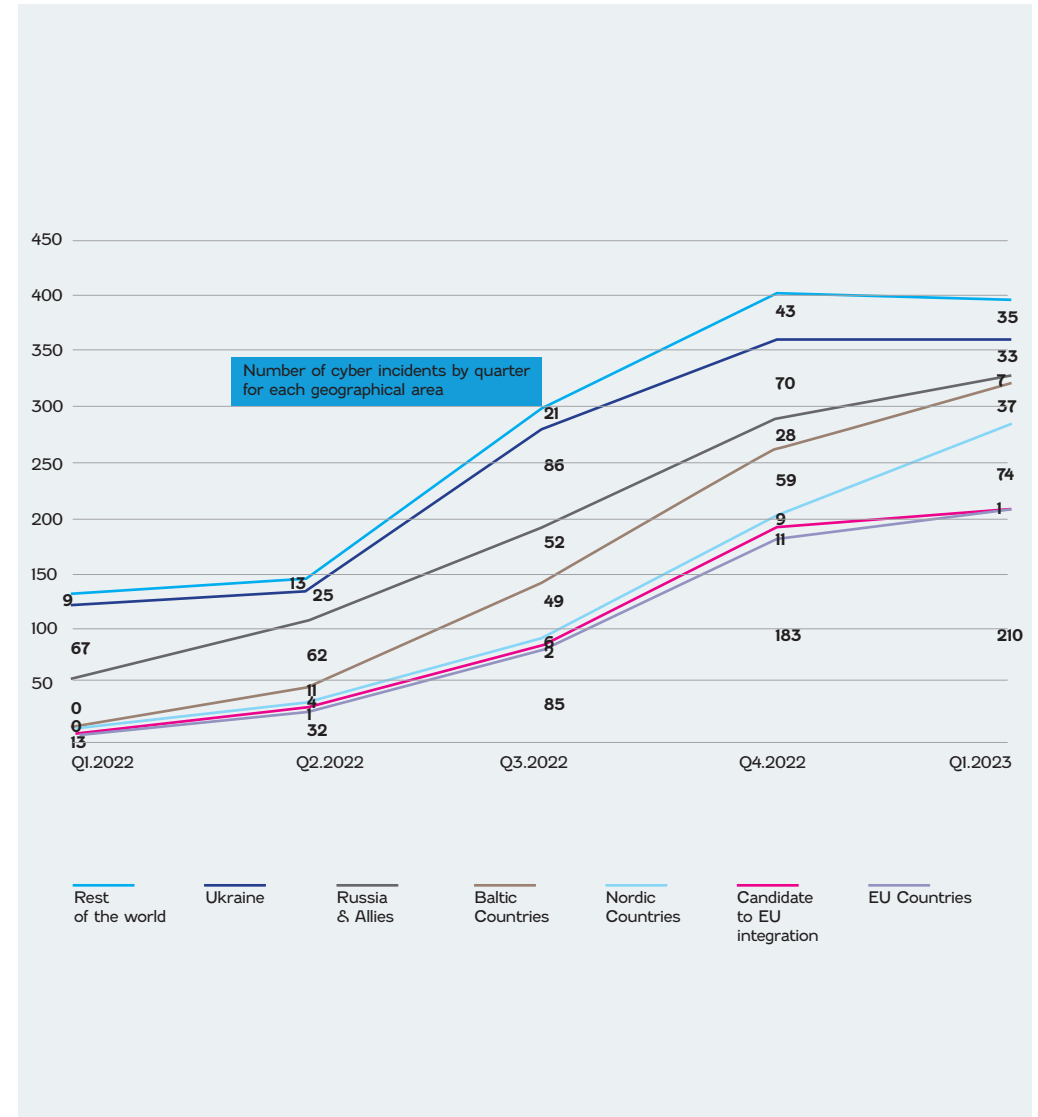
_AN INCREASE IN THE NUMBER OF ATTACKS COUPLED WITH A DIVERSIFICATION OF SECTORS: HEALTH, AVIATION AND THE FINANCIAL SECTOR ARE AMONG THE EMERGING TARGETS



This transition from targeted cyber warfare to hybrid cyber guerrilla warfare is also reflected in the «lateralisation» of the conflict to other geographical areas.

At the very beginning of the conflict, the majority of incidents only affected Ukraine, but EU countries have seen a sharp increase in conflict-related incidents since then.

FIGURE 8: TREND IN THE VOLUME OF INCIDENTS BY GEOGRAPHICAL AREA (GLOBAL SCALE)
European countries largely overtake Ukraine as victims of cyber attacks in the first quarter of 2023

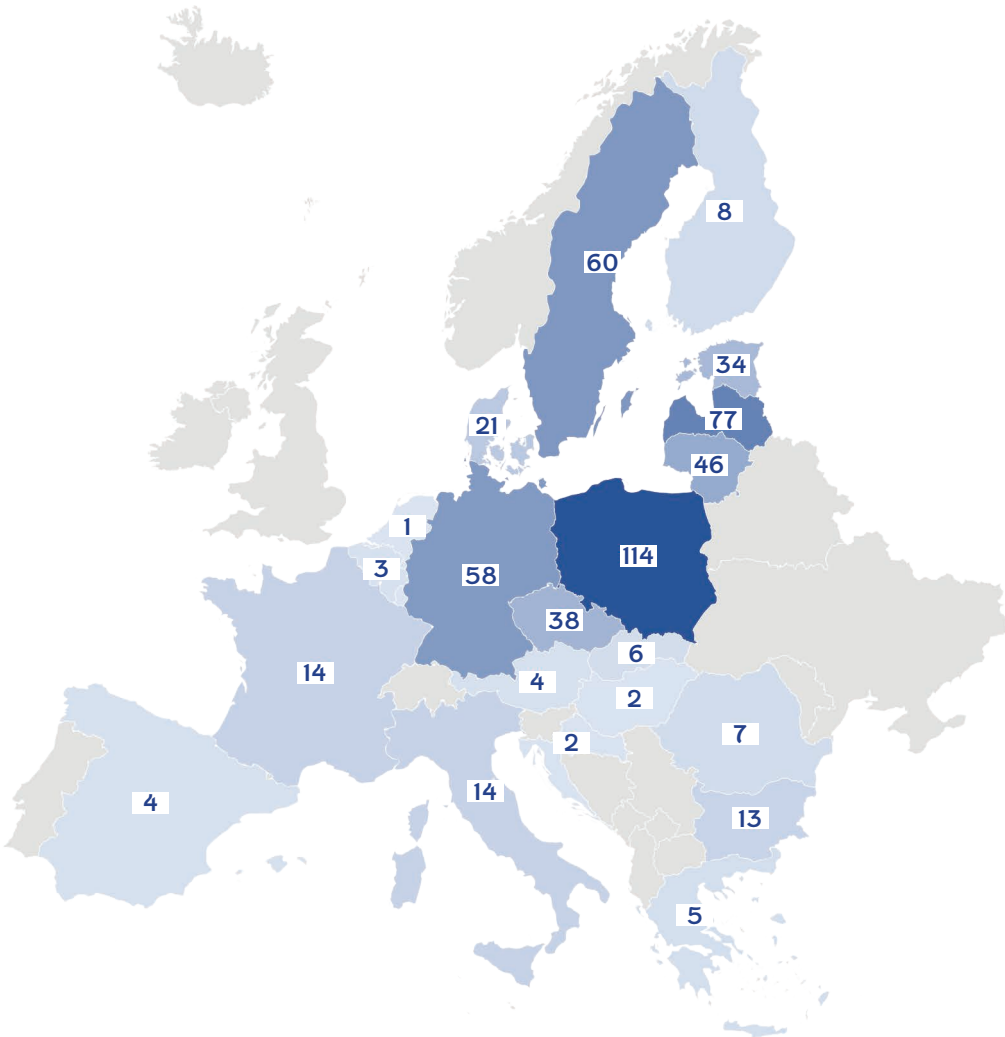


In the third quarter of 2022, there were almost as many conflict-related incidents in EU countries as there were in Ukraine (85 versus 86), and in the first quarter of 2023, the overwhelming majority of incidents were inside the European Union. The rate of incidents affecting EU coun-

tries also reflects a number of trends. Candidates for European integration such as Montenegro and Moldova are being increasingly targeted, Poland is constantly harassed, and the Baltic and Nordic countries are specifically targeted by war hackers.

FIGURE 9: DISTRIBUTION OF INCIDENTS BY COUNTRY AND GEOGRAPHICAL AREA (EUROPEAN SCALE)

Poland, Latvia, Sweden, among the most targeted countries after Ukraine and Russia



_FROM EPISODIC CYBER WARFARE TO PERMANENT CYBER GUERRILLA OPERATIONS

The shifting context of the conflict can therefore be summarised as a transition from a cyber-war focused on Ukraine and Russia to a high-intensity hybrid cyber-war.

_INFORMATION WARFARE: LOW OPERATIONAL IMPACT BUT A HIGH MORAL TOLL

It is true that DDoS attacks do not have a significant operational impact, unlike wiper attacks, which can destroy an adversary’s systems, and long-term strategic espionage, which can undermine the integrity of an adversary’s security apparatus. In terms of doctrine, it is important to remember that Russia does not necessarily consider the digital space in the same way as we do in the West from a strategic point of view. This point is further developed in the report. For example, we talk about cyber security and cyber defence, while Russia refers to information warfare. Information is seen not only as a means of action, but also as a space to be exploited. Cyber is therefore an ideal tool for harassing an adversary without engaging in direct confrontation, and Russia has understood this well. Some observers have asserted that the large pro-Russian hacktivist groups are directly controlled by the Russian military, and while there is no definitive evidence for these claims, the ultimate objective remains clear.

_CYBER-HARASSMENT SOWING CONFUSION AND ANXIETY

Pro-Russian hacktivist groups are now mostly attacking European countries that have taken clear positions or are acting in favour of Ukraine. And while their attacks do not have a major operational impact, as we mentioned above, the waves of DDoS attacks continue unabated. This systematic, low-impact harassment can sustain a climate of anxiety among security teams and decision-makers by lateralising the conflict beyond the borders of Russia and Ukraine at little cost. The objective is to occupy the European cyber space and cause alarm, with attacks on airports and hospitals for example, to divert attention from what is happening in Ukraine and prevent any intervention/assistance for the benefit of the aggressed nation. Acts of cyber warfare are still taking place in Ukraine – as we saw with the ATK256 (UAC-0056) attack against several Ukrainian public bodies on the anniversary of the conflict (February 23, 2023) – yet they are drowned out in the eyes of Westerners by constant cyber harassment. This cyber-diversion, which is either deliberate or has developed naturally as the conflict has evolved, is most visible in the countries targeted in the European Union, and notably Poland, the Baltic States and the Nordic countries.







Cyber Solutions by Thales

If you wish to discover more,
Please download the extensive report here:
<https://cyberthreat.thalesgroup.com/media-library/reports>



cyberdefencesolutions@thalesgroup.com

> cyberthreat.thalesgroup.com <    

THALES
Building a future we can all trust