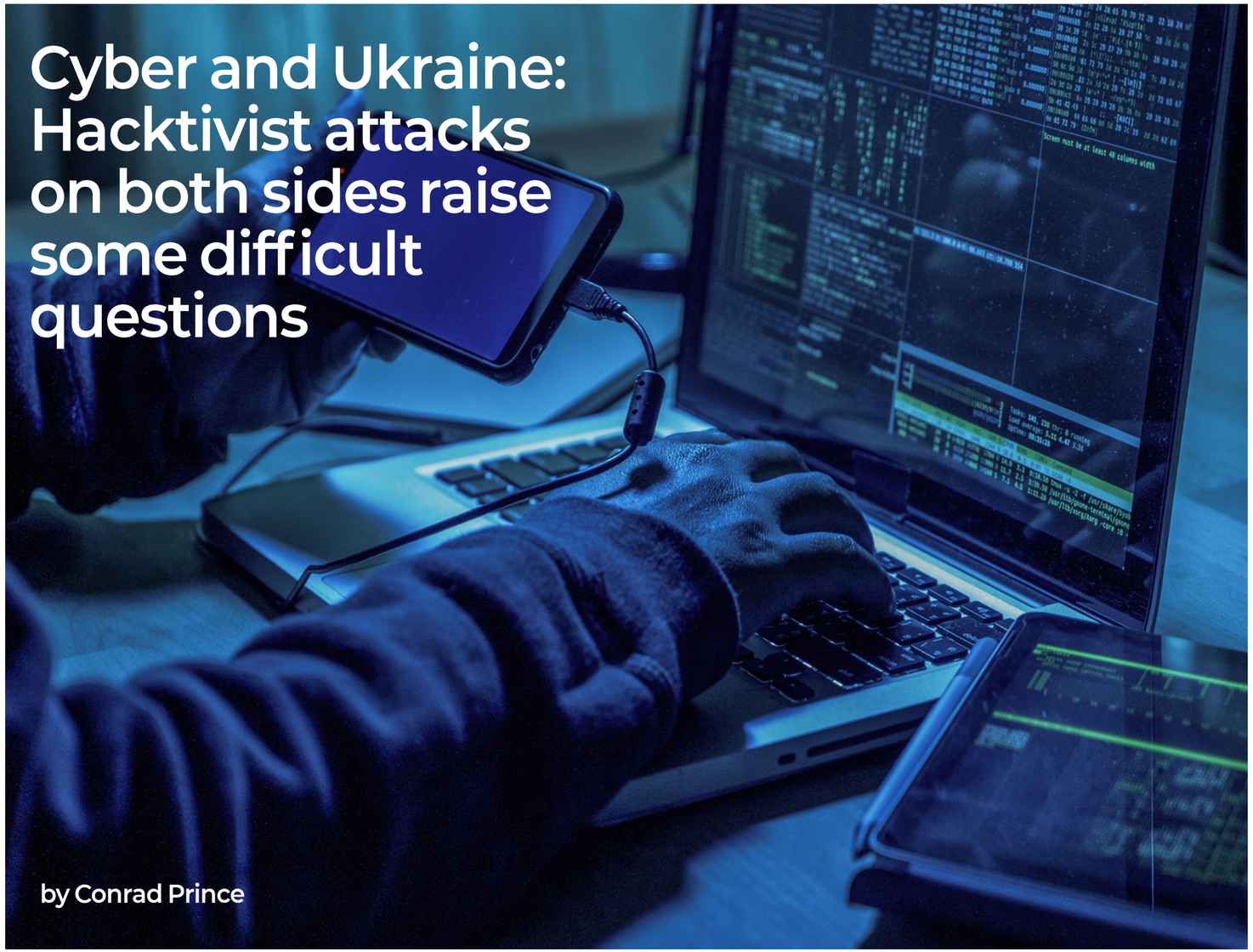
Summary

What is the role of non-state cyber groups in the Russia-Ukraine conflict and the implications of their actions at home and abroad?

Terrorism-related charges and convictions have increased in November 2022, returning to the levels observed in the first quarter of 2022. Pool Re Solutions assesses the latest open source and UK government data to suggest what trends we are likely to see in 2023. Read our analysis below.

We bring you the most up-to-date, significant, terrorism-related news, focusing on advanced market countries:

- The majority of convicted terrorists in Britain are radicalised online, study suggests.
- The number of far-right extremist inmates in Britain rises to highest ever level.
- Lockerbie bombing suspect is remanded in US custody.
- The arrest of 25 individuals accused of plotting to overthrow the German government.
- Islamic State supporters pledge allegiance to new leader.



Cyber and Ukraine: Hacktivist attacks on both sides raise some difficult questions

by Conrad Prince

Pool Re foreword

Although it is unlikely that cyber has been a decisive component of the Russian invasion of Ukraine, the conflict has seen significant involvement by non-state cyber actors, on both sides, including hacktivists, concerned citizens and even cyber criminals. On one side, various groups have expressed support for Russia and conducted cyber operations against Ukrainian and Western interests.

In response, entities such as the IT Army of Ukraine, which appears to have no formal status within the Ukrainian state, have launched cyber-attacks against Russian targets including banks and other civilian infrastructure.

It is likely that the practical impact of these attacks has been low; however, they are raising a number of questions around the legal status of different cyber actors and the threshold at which such activities might be defined as acts of terrorism.

Conrad Prince, Pool Re's senior cyber adviser, explores the role of non-state groups in the Russia-Ukraine conflict and the implications of their actions at home and abroad.

Introduction

Russia's illegal war on Ukraine continues to dominate the headlines with little sign of a positive resolution any time soon. It is a brutal conflict, with high military and civilian casualties and terrible physical destruction.

While there has been plenty of Russian state cyber activity linked to the invasion, there has not been any kind of 'cybergeddon'. If anything, the war has demonstrated the primacy of traditional kinetic capabilities in an armed conflict. But while cyber has not been militarily decisive, it has been notable for the extent to which non-state cyber actors have become involved on both sides.

Cyber and Ukraine: Hacktivist attacks on both sides raise some difficult questions (continued)

Non-state cyber actors in the Ukraine war

Ukraine has seen the widespread involvement of both hacktivist and cyber-crime groups rallying to one or other side in the conflict.

Early in the war, Conti, arguably the leading criminal ransomware group at the time, publicly came out in support of Russia. The group subsequently splintered as pro-Ukrainian members of the gang broke away and large volumes of information about the group was leaked online.

The hacker group Killnet has also expressed support for Russia, 'declaring war' on 10 countries. It has been linked to DDoS attacks (distributed denial of service operations flooding websites with traffic to bring them down) on 130 government and commercial websites in Lithuania,[2] attacks on Italy,[3] and on multiple US institutions including websites of airports and various government organisations.[4]

The criminal group Trickbot has apparently switched its attention to Ukraine on a level not previously seen, reportedly launching attacks against government and critical infrastructure, and launching mass phishing operations against Ukrainian civilians.[5]

However, non-state cyber attacks are not limited to supporters of Russia. Ukraine has also seen a widespread mobilisation of non-state cyber actors carrying out attacks on its behalf. Shortly after the invasion, the Ukrainian government announced the formation of the 'IT Army' of Ukraine, calling on Ukrainian civilian IT experts to conduct cyber operations against Russia on behalf of the state. The Government went on to direct the volunteer hackers to launch a cyber attack on the website of the Moscow Stock Exchange.[6]

The IT Army has reportedly attracted several hundred thousand followers and has continued to conduct operations against Russian targets, both governmental and civilian entities (such as banks). The Ukrainian Government claims that thousands of Russian online resources have been affected by Ukrainian hackers.[7]

Other groups have also rallied to the Ukrainian cause. The hacktivist group Anonymous has been a prominent supporter, claiming multiple cyber operations against Russian interests. And in advance of the invasion a Belorussian dissident group dubbed the Cyber Partisans claimed to have successfully launched a ransomware attack against the Belorussian railway system, aiming to hamper the transport of Russian troops to Ukraine.

There are indications of active support for Ukrainian non-state cyber operations elsewhere in Europe, including from cyber companies based in Estonia and a Ukrainian IT company that has relocated to Portugal. This may just be the tip of the iceberg. It is not easy to develop accurate statistics on this sort of cyber activity, but one institution monitoring the conflict has concluded that over 60% of the cyber operations observed in the conflict have been launched by hacktivist groups.[8]

Cyber and Ukraine: Hacktivist attacks on both sides raise some difficult questions (continued)

The real-world impact of these cyber operations is generally limited. Despite the melodramatic rhetoric of some perpetrators, the majority of successful attacks cause no more than short-term disruption. In many ways the impact is much more significant in propaganda and perception terms, rather than in practical reality.

What are the implications?

There are, though, some broader implications from this profusion of non-state cyber activity. There is nothing new about shadowy Russian hacktivists launching politically-motivated attacks on foreign states, going as far back as the extensive 2007 denial of service attacks on Estonia.[9]

But the potential of cybercriminals using ransomware to target perceived opponents of Russia feels more concerning than some DDoS attacks – given the damage done by recent ransomware attacks against critical infrastructure targets such as Colonial Pipeline[10] in the US and the Irish healthcare system.[11]

Moreover, there are some indications that the Russian state has generally sought to avoid escalating the conflict beyond Ukraine. However, hacktivist or criminal groups politically aligned to Russia may feel no such restraint and be much more willing to target the West, with potentially escalatory consequences.

Meanwhile, the hackers rallying to support Ukraine raise their own set of issues. The IT Army of Ukraine appears to have no official status – it is not a military formation, nor an official civilian government entity. It is a loose grouping of what are in effect hacktivists - but hacktivists that have been mobilised by the state, and, at least in the conflict's very early days, directed by it. And they are carrying out disruptive cyber-attacks against a foreign state, including targeting civilian infrastructure and organisations that are not subject to any international sanctions. Arguably these actions raise several legal issues and potentially go against internationally agreed norms of behaviour in cyberspace. So what should the West's response be, however much it may applaud the aims of these groups?

Furthermore, there is evidence that some of this activity is being conducted from within the EU.[12] Is it right that member states should tolerate hacktivist cyber-attacks being launched from their territory that may well be unlawful and contrary to agreed international norms? And if Western nations are seen to tacitly support Ukrainian hacktivist attacks on Russian civilian infrastructure, including banks and other businesses, does that risk encouraging and legitimising Russian hacktivist attacks on the equivalent Western institutions?

Finally, this also raises some interesting questions around terrorism. Non-state groups are carrying out politically motivated disruptive and potentially destructive acts (albeit with little impact so far), which it could certainly be argued are designed to influence and intimidate. Should such acts get to the point of achieving serious effect there is probably a question of whether they could be defined as terrorism, with all that that entails.

There are deep waters here. It may be that this proliferation and evolution of non-state cyber-attacks for political ends, with the challenging legal, political and ethical questions it brings, is one of the more significant aspects of the cyber conflict around Ukraine.

About the author:

Conrad Prince is Pool Re's senior adviser on cyber and terrorism. He is a Distinguished Fellow at the leading defence and security think tank, the Royal United Services Institute, and also advises a range of companies on cyber strategy. He spent most of a thirty year career in public service at GCHQ, the UK's cyber intelligence and security agency. He was deputy head of the agency for seven years. Following that he was the UK Government's first Cyber Security Ambassador, helping overseas governments develop their national cyber strategies and capabilities.

UK Terrorism Offence Data: December Update

by Becca Stewart Pool Re Threat Analyst

Key Points

- 10 individuals were charged or sentenced in the UK in relation to terrorist activity in November 2022, a sharp increase in comparison to the previous three months.
- The number of charges and sentences in November 2022 marks a return to the level of terrorist related legal cases observed in the first quarter of 2022. It is unlikely that represents an overall increase in the terrorist threat to the UK. Instead it is likely that November presents an outlier amongst the lower rates of terrorism-related legal activity observed throughout the year.
- In the first half of December the level of cases has dropped with two charges at present (14 December 2022). This is consistent with the low number of terrorism-related legal activity observed in December 2021.

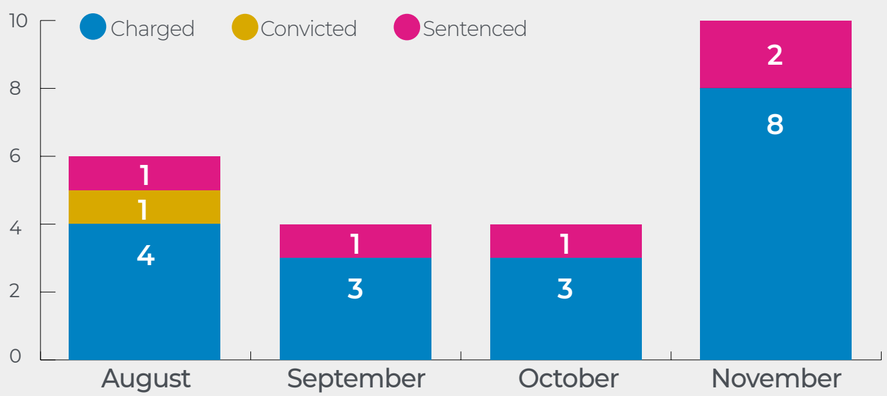
Insight into November's cases

A Derbyshire teenager, Daniel Harris, was convicted for encouraging terrorism through extreme right-wing videos he posted online. The videos reportedly glorified white supremacist murderers and called for an armed insurrection. He was also convicted for possession of a 3D printer with the intent to use it to manufacture 3D printed weapons for terrorist purposes.

There is a realistic possibility that Harris could also be extradited to the US for inspiring a mass shooting in Buffalo, New York. Payton Gendron killed 10 black people in a supermarket in Buffalo in May 2022, an incident which Harris celebrated in a video posted hours after the attack. Gendron included screenshots in his manifesto of Harris's videos calling for genocide against people of colour, and had previously commented on one of Harris's videos.

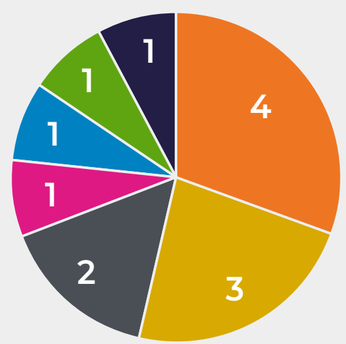
This case demonstrates the intent of radicalised individuals to manufacture 3D printed weapons in the UK for terrorist purposes. It is likely that there would be further attempts to construct similar weapons in 2023 as extremists attempt to circumvent restrictions surrounding firearms, explosive precursors and other weaponry.

The number of individuals charged, convicted or sentenced regarding terrorist activity

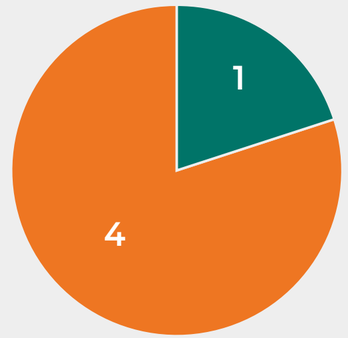


Source: Pool Re internal database

Number of people charged, convicted or sentenced for terrorism offences in November 2022



Number of people charged, convicted or sentenced for terrorism offences in October 2022



Note:
Several individuals in both months were involved with more than one offence so appear on the diagram multiple times.

More

UK Terrorism Offence Data: December Update (continued)

Home Office quarterly Counter Terrorism statistics

In December 2022, the Home Office issued its updated Counter terrorism statistics for the year ended September 2022.

Key statistics drawn from the reporting include.

- The 190 total arrests in the year ended September 2022 remains consistent with the previous 12 months.
- 16% of arrests were individuals aged 17 and under, the highest proportion of children arrested for terrorism in a 12-month period on record. A heightened level of young people arrested for terrorism was seen consistently throughout 2022, this trend is likely to continue into 2023.
- Dissemination of terrorist publications remains the most prominent terrorism-related charge. The majority of charges are related to the distribution of propaganda via messaging, through social media and on online forums.
- The number of Islamist extremists in custody in Great Britain has remained stable in recent years; however, the number of individuals in custody for right-wing extremism increased by 35% in the year ended September 2022.
  - It is likely that the trend of increasing numbers of extreme right-wing convictions would continue in 2023.
  - This might not necessarily mean the amount of extreme right-wing terrorist activity would be significantly increased, instead this would highly likely be the result of greater police and public resource being allocated to understand and mitigate the threat from right wing extremism. In essence – if more resource is allocated to uncovering threats, the likelihood of uncovering a greater number of threats would increase.
  - The increase in far-right convictions has reinforced the call for concern regarding right-wing extremism by the MI5 Director General and the UK Minister for Security and Borders over the past 12 months.
  - This data is consistent with a recent study regarding the high volume of British people being radicalised towards online terrorism in the online environment. More can be read about this study in the news roundup below.

News Roundup

by Oliver Hair Pool Re Junior Threat Analyst

UK: Majority of convicted terrorists are radicalised online

A recent study by the Ministry of Justice has found that the majority of convicted terrorists in Britain were radicalised online.[13] The study examined official risk assessments of every convicted terrorist in prison since 2010. From 2019-21, 92% of those convicted were radicalised wholly or in part online. The study also revealed that 42% of those radicalised online between 2010 and 2021 had significant mental health issues, neurodivergence and/or personality disorder. Autism Spectrum Condition (ASC) and depression were the most common conditions found amongst those radicalised primarily online.[14]

For those primarily radicalised online, the most common type of plots included the use of improvised explosive devices (IEDs, 65%), bladed weapons (24%), or Vehicle as a Weapon (12%). Their plots, however, were found less likely to succeed.

This challenges previous assessments that internet radicalisation has enabled terrorist actors to evade the security services and police. Instead, it is likely that the online traces of threat actors make it more difficult for individuals to progress in attack planning by providing greater opportunity for disruption by police or security services.[15] It is highly likely that the internet will remain the primary mode of radicalisation for terrorist actors in Britain; however, the number of those who would turn to violence remains uncertain.

News Roundup (continued)

UK: Number of far-right extremist inmates rises to highest ever level

New Home Office figures reveal that there were 190 counter terrorism related arrests in the year to September 2022 and the number of far-right extremist in prison has risen to its highest ever level.[16] In the same period, the proportion of terrorist inmates holding Islamist-extremist views has fallen to its lowest level on record.[17] While MI5 Director General Ken McCallum revealed last month that Islamist-extremism still accounts for roughly three-quarters of the security agency's caseload, he also warned that extreme right-wing terrorism is "here to stay".[18] It is therefore assessed as likely that far-right extremist related convictions will continue to rise in the near to medium-term. The figures also reveal that under-18's currently account for 16% of all arrested terror suspects; a 3% increase on the previous year.[19] It is highly likely that children and young adults will remain at risk of being radicalised online in the near future, particularly from far-right ideologies.

December 1988: Some of the wreckage of Pan Am Flight 103 after it crashed onto the town of Lockerbie in Scotland, on 21st December 1988. Photo by Bryn Colton/Getty Images

UK: Lockerbie bombing suspect in US custody

A Libyan man alleged to have built the bomb which destroyed Pan Am flight 103 over Lockerbie in 1988 has been remanded in US custody, Scottish authorities have reported.[20] The bomb killed all 259 passengers and crew on board, while another 11 were killed on the ground by the wreckage. It remains the deadliest terrorist attack to have ever taken place on British soil.[21] The suspect, Abi Agila Musad, was named in 2020 by the US Department of Justice as the man who had constructed the bomb.[22] The suspect was reportedly Colonel Gaddafi's chief bomb-maker and ordered to fly to Malta in December 1988 to prepare the device. Five years ago, Musad reportedly confessed to being involved in the plot to blow up the flight whilst serving a prison sentence in Libya.[23] He is due to face a detention hearing later in December.

News Roundup (continued)

GERMANY: 25 individuals arrested for plotting to overthrow the government

On 07 December, twenty-five people were arrested in Germany on suspicion of plotting to overthrow the government. The group allegedly planned to storm parliament and seize power by "military means and violence against state representatives".[24] Aristocrat, Heinrich XIII Prinz Reuss, was allegedly the leader of the plot and had been planning the coup since November 2021.[25] It is likely that the group's affiliates number far higher than the 25 individuals currently in custody and that further arrests will be made in the near future.[26] Those arrested include members of the right-wing Reichsbürger movement, a judge, and a celebrity chef. A serving member of the German Special Forces was also arrested, illustrating the threat posed by right-wing extremism within the armed forces and by those with access to weapons and military expertise. As the UK government's intelligence watchdog has recently warned, there is a realistic possibility that right-wing extremists in the UK would seek to infiltrate the military because of their interest in and capability to access weapons.[27]

The plot illustrates the growing threat posed by far-right radicalism throughout advanced market countries. Germany has seen several violent attacks linked to the far right and struggled with a wave of home-grown extremism in recent years. In 2020, a 43-year-old far-right extremist killed nine people in attacks on two shisha bars in Hanau, a city in western Germany.[28] Outside of Germany, recent attacks in Dover, UK and Slovakia have shown the continued threat posed by right-wing extremism in the UK and wider Europe. Extreme right-wing actors have previously demonstrated the intent and capability to conduct attacks in the UK and it is likely that this will continue to be a heightened threat in the next 12 months. It is highly likely that individuals will remain at risk of becoming radicalised by similar ideologies online as the lasting effects of lockdown, the cost-of-living crisis, and immigration crisis continue to be felt.

Police officers work during a raid in Berlin, Germany, on December 07, 2022. Photo by Abdulhamid Hosbas/Anadolu Agency via Getty Images

WORLD: Islamic State supporters pledge allegiance to new leader

Several Islamic State (IS) supporters and fighters pledged allegiance to their new leader last month following an announcement of the death of "Caliph" Abu al-Hasan al-Hashimi al-Qurashi. The group later announced his successor, Aby al-Husayn al-Husayni al-Qurashi, through a propaganda campaign reportedly to show the group's strength.[29] It is reported that the group's former leader was killed in an operation carried out by rebels of the Free Syrian Army in southern Syria in mid-October. IS emerged out of the civil war in Iraq and grew to control large areas of Iraq and Syria in 2014. The majority of the group's control was brought to an end in Iraq in 2017 and Syria in 2019.[30]

It is likely that the death of IS' second leader in a year comes at a challenging time for the group. Whilst the group has demonstrated the intent and capability to conduct sporadic attacks in Afghanistan and parts of Syria, its operational tempo reportedly continues to decline in Iraq.[31] The pledges of allegiance to the group's new leader have now shown a stronger presence in Africa, particularly in Mali and other areas of the Sahel.[32] Whilst it is highly unlikely that terrorist actors across Africa will pose a direct threat to the UK mainland at this time, it is likely that sections of the African continent will provide an increasingly permissive environment for terrorist groups to conduct operational activity. As such, there is a realistic possibility that continued expansion of Islamic-related terrorism across Africa could lead to a heightened threat to the UK mainland in the long term and/or attack(s) on British interests overseas. Whilst it is currently unlikely that terrorist actors in the UK would have the intent to conduct terrorist related activity on behalf of those on the African continent in the near future, the training of overseas operatives, returning fighters, and the exploitation of migrant networks could facilitate the travel of malicious actors into the UK.

References

Threat Overview

1 Conrad Prince is Pool Re's senior adviser on cyber and terrorism. He is a Distinguished Fellow at the leading defence and security think tank, the Royal United Services Institute, and also advises a range of companies on cyber strategy. He spent most of a thirty year career in public service at GCHQ, the UK's cyber intelligence and security agency. He was deputy head of the agency for seven years. Following that he was the UK Government's first Cyber Security Ambassador, helping overseas governments develop their national cyber strategies and capabilities.

Cyber and Ukraine: Hacktivist attacks on both sides raise some difficult questions ?

2 https://www.wired.co.uk/article/russia-hacking-xaknet-killnet

3 Russian hackers declare war on 10 countries after failed Eurovision DDoS attack: IT PRO

4 US airports' sites taken down in DDoS attacks by pro-Russian hackers (bleepingcomputer.com)

Russian hackers knock US state government websites offline: CNN Politics

5 Unprecedented Shift: The Trickbot Group is Systematically Attacking Ukraine (securityintelligence.com)

6 https://www.theregister.com/2022/08/11/black_hat_hacktivists

Moscow Exchange, Sberbank Websites Knocked Offline—Was Ukraine's Cyber Army Responsible? (forbes.com)

7 Ministry of Digital Transformation: Telegram

8 Cyber Threats Landscape: CyberPeace Institute

9 2007 cyberattacks on Estonia: Wikipedia

10 The Colonial Pipeline Hack Is a New Extreme for Ransomware: WIRED

11 Cyber attack had 'devastating impact' on Republic's health service: The Irish News

12 They Fled Ukraine to Keep Their Cyber Startup Alive. Now, They're Hacking Back: WSJ

Inside Ukraine's cyber guerrilla army: DW – 03/24/2022

UK: Majority of convicted terrorists are radicalised online

13 Internet and radicalisation pathways: technological advances, relevance of mental health and role of attackers : GOV.UK (www.gov.uk)

14 Internet and radicalisation pathways: technological advances, relevance of mental health and role of attackers: GOV.UK (www.gov.uk)

Home Office terror figures flag rise in number of far-right extremist inmates: ITV News

15 Most convicted terrorists radicalised online, finds MoJ-backed study - UK security and counter-terrorism: The Guardian

UK: Number of far-right extremist inmates rises to highest ever level

16 Operation of police powers under the Terrorism Act 2000, quarterly update to September 2022: GOV.UK (www.gov.uk)

17 Statistics show continued rise in youth arrests for terrorism offences:Counter Terrorism Policing

Home Office terror figures flag rise in number of far-right extremist inmates:ITV News

18 Ibid.

19 Rise in youth arrests for terrorism offences: Counter Terror Business

UK: Lockerbie bombing suspect in US custody

20 Lockerbie bombing suspect in US custody: BBC News

21 Lockerbie bombing suspect in US custody: BBC News

22 Lockerbie bombing suspect due to appear in US court: BBC News

23 Lockerbie bombing suspect makes first US court appearance: The Independent

GERMANY: 25 individuals arrested for plotting to overthrow the government

24 Germany arrests 25 accused of plotting coup: BBC News

25 The far-right plot to overthrow Germany: Financial Times (ft.com)

26 Germany expects more arrests after coup plot swoop : Reuters

27 The far-right plot to overthrow Germany: Financial Times (ft.com)

German 'coup' prompts push to purge extremism in police and military (thenationalnews.com)

Right-wing extremists seek to infiltrate military 'for weaponry' (telegraph.co.uk)

28 Germany shooting- 'Far-right extremist' carried out shisha bars attacks: BBC News

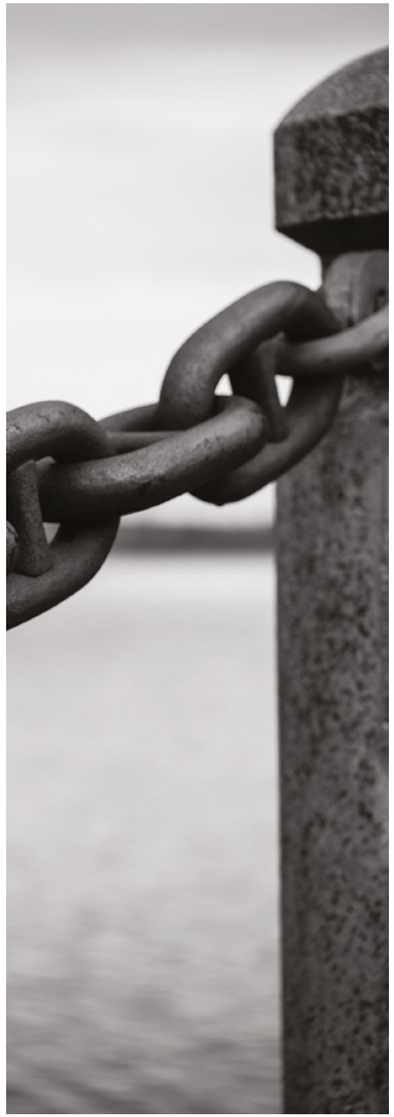
WORLD: Islamic State supporters pledge allegiance to new leader

29 Pro-IS Media Units Release Videos Promoting the Outpouring of Pledges from Fighters to New 'Caliph', Jihadist Threat - Multimedia: Jihadist News, Articles (siteintelgroup.com)

30 Islamic State leader blew himself up after being surrounded, Syrian fighter says; World News: Sky News

31 ISIS leader's death raises intriguing questions: Middle East Institute (mei.edu)

32 Calibre Obscura on Twitter: "#Sahel: A Bay'ah photoset showing a fairly massive amount of ISIS militants in #Mali was released. Militants armed with ZU-23-2 autocannon, ZPU-2 dual autocannon, and of course a wide variety of AK/PK variants. https://t.co/61vRAq2Y16" / Twitter



POOL Re SOLUTIONS

Risk Awareness **Risk Modelling** **Risk Management**

Understanding risk, enabling resilience

Whilst the human cost of terrorism is devastating, the financial impact an incident can have on communities, businesses and economies is generally greater than most realise.

At Pool Re we understand that terrorism is a significant multi-faceted peril that can expose businesses in a complex way. Like many other catastrophic perils, terrorism is a challenge which requires a collaborative approach.

We have been the UK's leading terrorism reinsurer for over a quarter of a century. During this time our *SOLUTIONS* division have developed a specialist team of experts who can work with you to help you and your Policyholders understand and manage the terrorism threat.

We believe all organisations and businesses can benefit from a better understanding of the terrorism risk solutions available.

To find out more about Pool Re *SOLUTIONS* and how your organisation can take advantage of this service please contact us at:
solutions@poolre.co.uk

Threat level

	Critical: an attack is highly likely in the near future	Severe: an attack is highly likely	Substantial: an attack is likely	Moderate: an attack is possible but not likely	Low: an attack is highly unlikely
Threat from terrorism to the UK:			●		
Threat from Northern Ireland related terrorism to Northern Ireland:			●		

Government advice

Click a logo for more information

ACT ACTION COUNTERS TERRORISM

CPNI Centre for the Protection of National Infrastructure

CSSC Cross-sector Safety and Security Communications

SECURITY SERVICE MI5

COUNTER TERRORISM POLICING UK Protect

SEE IT. SAY IT. SORTED.

RUN HIDE TELL

National Cyber Security Centre a part of GCHQ