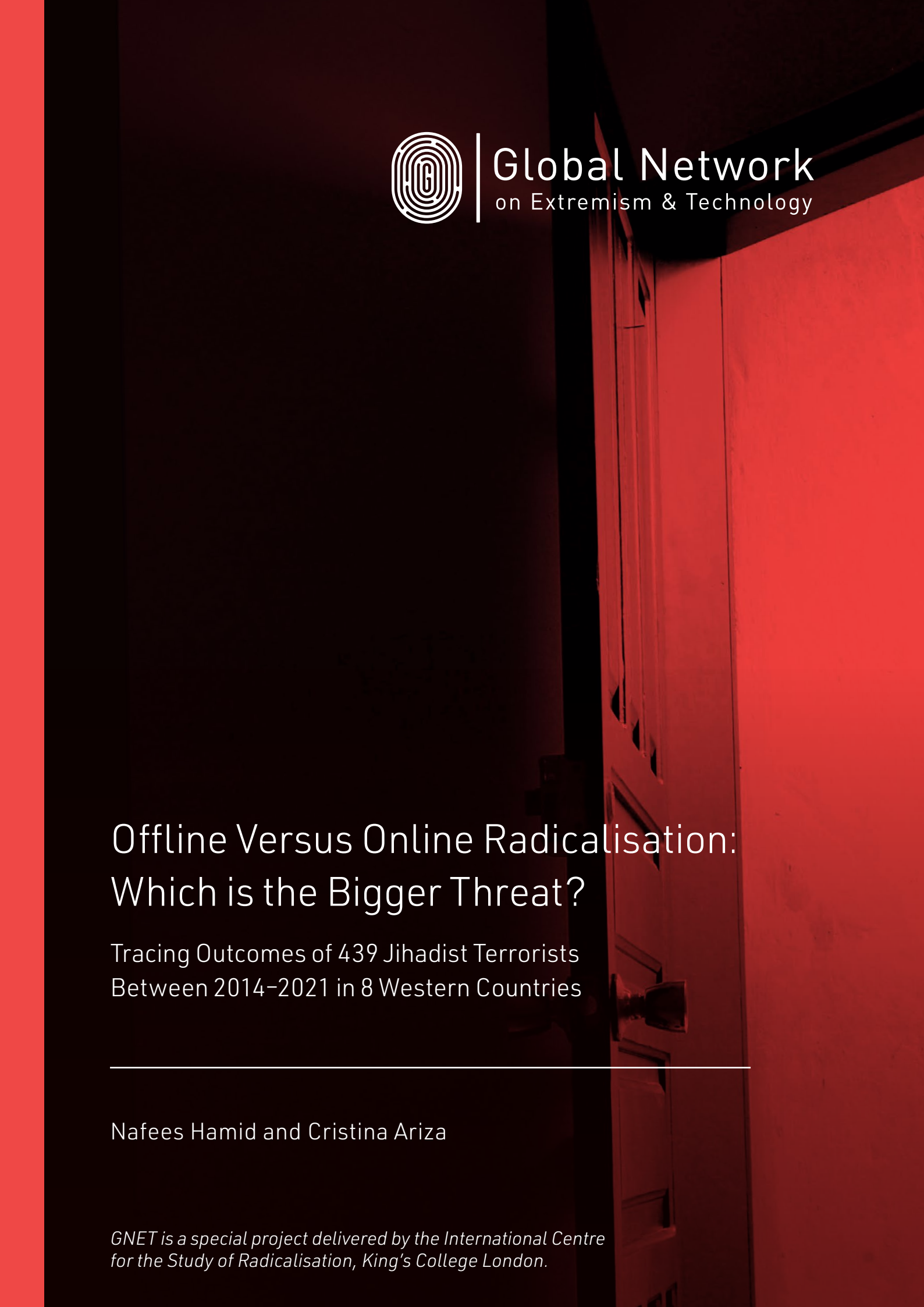

Global Network
on Extremism & Technology

Offline Versus Online Radicalisation: Which is the Bigger Threat?

Tracing Outcomes of 439 Jihadist Terrorists Between 2014–2021 in 8 Western Countries

Nafees Hamid and Cristina Ariza

GNET is a special project delivered by the International Centre for the Study of Radicalisation, King's College London.

The authors of this report are
Nafees Hamid and Cristina Ariza

The Global Network on Extremism and Technology (GNET) is an academic research initiative backed by the Global Internet Forum to Counter Terrorism (GIFCT), an independent but industry-funded initiative for better understanding, and counteracting, terrorist use of technology. GNET is convened and led by the International Centre for the Study of Radicalisation (ICSR), an academic research centre based within the Department of War Studies at King's College London. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing those, either expressed or implied, of GIFCT, GNET or ICSR.

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.

Executive Summary

Question: Are those radicalised offline or online more of a threat? Which group is harder to detect, more successful in completing attacks, and more lethal when they do so? Is the pattern different for youth versus older perpetrators and for men versus women? This report investigates these questions.

Database: We created a database containing 439 perpetrators involved in 245 attacks between 1 January 2014 and 1 January 2021. It includes every publicly known completed attack and an extensive sampling of thwarted attacks. Attacks were all jihadist-linked in eight Western countries: Australia, Austria, Belgium, France, Germany, Spain, the United Kingdom and the United States.

Type of radicalisation: In our database, radicalisation primarily happens offline; over half the individuals in our database had been radicalised via offline networks.

Success and lethality: Individuals who were radicalised offline were three times more likely than individuals radicalised online to complete an attack successfully. Those radicalised offline are 18 times more lethal than individuals in the online category. Those radicalised online are almost eight times more likely to fail than to succeed.

Group attacks: Individuals who were radicalised offline are almost three times more likely to attack or plot in groups than individuals radicalised online.

Success of group attacks: While groups were more likely to be thwarted by the police than to succeed (regardless of how individuals had been radicalised), successful groups of people radicalised offline were more lethal than their lone actor counterparts (15%).

Family and friends: Some 87% of those with radicalised friends and 74% with radicalised relatives plotted or attacked together.

Foreign fighters: Foreign terrorist fighters (FTFs), who were mostly radicalised offline, have the same success rate as non-FTFs. But success rate increases if they have spent more than a year in a terrorist training location.

Age: Online radicalisation is on the rise for young people (born from the 2000s onwards), although most individuals, including young people, are still radicalised offline.

Gender: Women appear to be more likely to have been radicalised online.

Bottom line: Those radicalised offline are greater in number, more successful in completing attacks and more deadly than those radicalised online.

Overview

Governments, social media companies and the general public are becoming increasingly concerned about the threat of those who are radicalised online and turn to violent extremism. However, the evidence base for this concern is not fully formed. For instance, it is not yet clear if those who are being radicalised offline are still the greater threat. It is particularly important to explore this issue empirically, as large amounts of material resources from both the public and the private sectors may be redirected from offline to online initiatives. This report seeks to explore the differences in outcomes for those who have been primarily radicalised offline versus those radicalised online.

It does so by creating a new database with a novel coding system. The database contains information regarding every completed and most of the thwarted jihadist-linked attacks in eight Western countries (Australia, Austria, Belgium, France, Germany, Spain, the United Kingdom and the United States) over a seven year period from 1 January 2014 to 1 January 2021. The database contains 245 completed or thwarted attacks by some 439 individuals. For every perpetrator, the database contains information on how they were radicalised (mostly online; mostly offline; both; "asocially" online; and unknown – see chart in methodology section for definitional breakdown). It also contains information on target type and location, outcome of attack (completed; thwarted), lethality of attack (deaths; injuries), lone/group factors, mode of attack (bomb; shooting; knife; and so on), terrorist organisational connections (inspired or orchestrated by IS or al-Qaeda or another group), demographics of attackers (gender; age; education; ethnic origin; socio-economic status; and so on).

The sample of perpetrators and attacks was drawn from existing databases for terrorist attacks, including the START Global Terrorism Database, the George Washington's Program on Extremism database of attacks in the West, the French National Assembly's database of terrorist attacks in France, the UK's Independent Reviewer's database of Terrorism, the database of plots in Spain from Observatorio Terrorismo and Seguridad Internacional, and more. In addition to the information contained in these databases, we identified further attacks and plots through open-source research. This included access to court documents from each of the countries in the database. Moreover, we conducted dozens of interviews with police investigators, family members and friends of attackers, lawyers and others close to the cases.

Our findings suggest that the primary threat comes from those who have mostly been radicalised offline. More than half of the individuals in our database were radicalised mostly offline versus a significantly smaller number who were radicalised mostly online (54% vs 18%). Individuals radicalised mostly offline were significantly more likely to complete their attacks than those who were radicalised online (29% vs 12%). However, we found that the number of people being radicalised

online has increased over the last seven years, primarily in the youth demographic. Nonetheless, even in this demographic online radicalisation has not surpassed offline radicalisation.

Cases of online asocial radicalisation (by which we mean exposure to online propaganda with no known social interaction) accounted for only 2% of cases. Foreign terrorist fighters (FTFs) were equally as likely to carry out their attacks as non-foreign terrorist fighters (29% and 28%, respectively). More than 60% of completed attacks were committed by lone actors (67%). The best completion rate was for individuals who were radicalised offline and acted alone (60% completed an attack). Most individuals fitting this profile were either known to the police and/or under surveillance (68%) and had a criminal record or had been imprisoned (74%). A significant proportion of them were foreign fighters (26%). Nonetheless, 35% had radicalised friends or family even though they attacked alone.

Groups, regardless of radicalisation setting, achieved a significantly lower completion rate (15%). Even those who radicalised offline but attacked in groups had a low completion rate (19%), which is three times lower than lone actors who were radicalised offline but completed their attacks.

Yet people who had been radicalised offline acting in groups were 15% more lethal than when they attacked alone. Under half of these group actors were under surveillance or known to counter-terror (CT) police (44%, 1.5 times less likely to have been under surveillance or known to CT police than offline-radicalised lone actors who completed their attacks) or had been in prison previously (47%). People who had been radicalised online, both singly and in groups, accounted for only 12% of successful attacks.

Unlike other studies, our database consists of only those who have completed an attack or were thwarted before being able to do so. Therefore, it gives a more accurate picture of the actual threat landscape over seven years in eight Western countries than studies based on surveys or less representative sampling techniques. Our findings show that the primary threat still comes from those who have been radicalised offline. Offline-radicalised individuals are greater in number, better at evading detection by security officials, more likely to complete a terrorist attack successfully and more deadly when they do so.

Contents

1 Introduction

Even before the establishment of Islamic State's so-called caliphate in mid-2014, there was growing concern about the level of radicalisation taking place online. Media-fodder expressions like "bedroom radicalisation" fuelled public fears about young men and women being groomed online to join militant groups in foreign lands. Indeed, there was plenty of anecdotal evidence that, before making their way overseas, people were in contact with members of jihadist groups online. In the years that followed, many people who attempted to carry out or succeeded in carrying out jihadist-linked terrorist attacks domestically were found to have spent a lot of time consuming propaganda and communicating with members and/or supporters of jihadist groups.

As a result, considerable scrutiny came down on social media companies and other online platforms that made accessing terrorist-group materials and members too easy. After public and political pressure, many of these platforms imposed strict user guidelines that allowed the companies to remove content and profiles associated with terrorist groups. The underlying idea was that making it difficult to access the material and members of terrorist groups would curb the rate at which such groups could recruit new adherents.

Even at its outset this approach had its detractors. Some argued that if radicalisation were primarily taking place online, we should expect to see even geographical distribution of recruitment rates (or at least a correlation with the distribution of access to the Internet).[1] However, the presence of "hotspots" belied these inferences. For instance, 45% of Belgian FTFs came from Brussels despite it containing only 17% of the country's population.[2] And most of those FTFs came from just a few neighbourhoods in the "croissant pauvre" region of the city. Findings such as this indicated that offline factors were playing a significant role in radicalisation.

Many experts agreed that, in the modern context, both online and offline factors were important for understanding radicalisation patterns. However, what is distinguishable is the setting in which individuals were primarily recruited. For example, a person may have undergone significant life stressors, such as coming from a broken family, living in a marginalised neighbourhood or falling into a life of crime. All of these experiences might make them antagonistic towards their society and its institutions, leading to feelings of disaffection. Such an individual may then spend significant time online where they encounter a member of IS who builds a relationship with them over months and eventually convinces them to come to Syria.

1 Clare Ellis and Raffaello Pantucci, "Friends, Sponsors and Bureaucracy: An Initial Look at the Daesh Database", 3 May 2016, https://rusi.org/explore-our-research/publications/commentary/friends-sponsors-and-bureaucracy-initial-look-daesh-database/

2 Kristof Clerix, "Zeven op de tien Belgische Syri strijders zijn tieners of twintigers" ["Seven out of Ten Belgian Fighters in Syria are Teenagers or in Their Twenties"], Knack, 31 August 2016, https://www.knack.be/nieuws/belgie/zeven-op-de-tien-belgische-syriestrijders-zijn-tieners-of-twintigers/article-normal-746451.html?cookie_check=1565032300

At first glance, this seems like an example of how hard it is to tease apart offline and online factors in the radicalisation process. However, careful theorising should disentangle susceptibility from setting.[3] The offline factors presented in this example constitute the elements that increase a person's susceptibility to radicalisation; that is, what makes them more likely to get recruited if exposed to recruitment efforts. The online relationship and grooming by the IS member represents the setting of their radicalisation; that is, *where* they are recruited. In this example, we can say that the person was radicalised online. Offline settings could be prisons, mosques or even boxing gyms. In some cases, a person may start their process in one setting and then transition to the other or even be engaged in both settings equally.

It is the job of forensic investigators, the police and researchers to reverse engineer the pathway of radicalisation that an individual took. These investigations may reveal that the setting of a person's radicalisation primarily took place online, offline or both, or it may remain unknown. As with most forensic investigations, the evidence is often patchy and boundaries between mostly online and mostly offline can be fuzzy. However, even with this caveat in mind, it is still worthwhile to ask whether the setting of a (would-be) terrorist's radicalisation affects their trajectory. For instance, are those who are primarily radicalised online as opposed to offline more likely to get caught before their attempted attack? Are they more likely to attack in groups rather than alone? Are they more lethal when they complete an attack? These are some of the questions that this report will investigate.

3 Noemie Bouhana, "The Moral Ecology of Extremism: A Systemic Perspective", UK Commission for Countering Terrorism, July 2019. https://www.gov.uk/government/publications/the-moral-ecology-of-extremism-a-systemic-perspective

2 Methodolgy

The authors compiled a sample of 439 individuals who were involved in 245 completed and thwarted jihadist terrorist attacks between 1 January 2014 and 1 January 2021 in eight Western countries (Australia, Austria, Belgium, France, Germany, Spain, the United Kingdom and the United States). The authors selected the sample of countries based on their ability to consult sources in languages other than English (Spanish, French and German) and based on previous research undertaken for ARTIS International examining the prevalence of jihadist recruiters, which is why this database does not include data from other relevant Western countries that have suffered significant levels of terrorist activity, including Canada, the Netherlands and Sweden.

The sample of perpetrators and attacks was drawn from existing databases in the literature on terrorist attacks, including the START Global Terrorism Database;[4] Vidino, Marone and Entenmann's database of attacks in the West;[5] Hegghammer and Nesser's compilation of attacks and plots in the West;[6] Bergen, Schuster, and Sterman's report on IS in the West;[7] the court cases collected by the George Washington Program on Extremism;[8] Kurzman's report on Muslim Americans involved in extremism;[9] the collection of American cases by John Mueller;[10] Fenech and Pietrasanta's report for the French National Assembly about terrorist attacks in France;[11] Holman's compilation of terrorist incidents in France;[12] the website of the Counter-Terrorism Division of the Crown Prosecution Service;[13] annual reports by the UK's Independent Reviewer of Terrorism Legislation;[14] Andrew Zammit's research on terrorist plots in Australia;[15] Johannes Saal's book *The Dark Social Capital of Religious Radicals* for terrorist attacks and plots in Austria and Germany;[16] and the list of plots in Spain from Observatorio Terrorismo[17] and Seguridad

4 START Global Terrorism Database, https://www.start.umd.edu/gtd/
5 Lorenzo Vidino, Francesco Marone, Eva Entenmann, "Fear Thy Neighbor, Radicalization and jihadist attacks in the West", George Washington Program on Extremism, 2017, https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/FearThyNeighbor%20RadicalizationandJihadistAttacksintheWest.pdf
6 Appendix to Thomas Hegghammer and Petter Nesser, "Assessing Islamic State's Commitment to Attacking the West", Perspectives on Terrorism (2015). Last updated on 6 July 2015. http://www.terrorismanalysts.com/pt/index.php/pot/article/downloadSuppFile/440/21
7 Peter Bergen, Courtney Schuster, David Sterman, "ISIS in the West: The new faces of extremism", New America, 2015, https://www.jstor.org/stable/resrep10495
8 The Cases, George Washington Program on Extremism, https://extremism.gwu.edu/cases
9 Charles Kurzman, "Muslim-American involvement with violent extremism", Triangle Center on Terrorism and Homeland Security, 2016, https://kurzman.unc.edu/files/2016/02/Kurzman_Muslim-American_Involvement_in_Violent_Extremism_2015.pdf
10 John Mueller, "Terrorism since 9/11. The American Cases", 2019, https://politicalscience.osu.edu/faculty/jmueller/since.pdf
11 Georges Fenech, Sébastien Pietrasanta, "Rapport faitau nom de la commission d'enquête relative aux moyens mis en œuvre par l'État pour lutter contre le terrorisme depuis le 7 janvier 2015", 2016, http://www.assemblee-nationale.fr/14/pdf/rap-enq/r3922-t1.pdf
12 Timothy Holman, "The Swarm: terrorist incidents in France," The Jamestown Foundation, Terrorism Monitor Volume 13(21), 2015, https://jamestown.org/program/the-swarm-terrorist-incidents-in-france/
13 https://terrorismlegislationreviewer.independent.gov.uk/
14 https://www.cps.gov.uk/crime-info/terrorism/counter-terrorism-division-crown-prosecution-service-cps-successful-prosecutions-2016
15 Andrew Zammit, "Australians charged under Joint Counter-Terrorism Team operations since 2013", Andrew Zammit, 25 August 2015, https://andrewzammit.org/2015/08/25/australians-charged-under-joint-counter-terrorism-team-operations-since-2013/
16 Johannes Saal, *The Dark Social Capital of Religious Radicals: Jihadi Networks and Mobilization in Germany, Austria and Switzerland 1998–2018*, https://link.springer.com/book/10.1007%2F978-3-658-32842-9
17 "Bases de datos: operaciones policiales antiyihadistas en España", Observatorio Terrorismo, https://observatorioterrorismo.com/bases-de-datos/operaciones-policiales-antiyihadistas-en-espana-2/

Internacional.[18] In addition to the information contained in these databases, the authors identified further attacks and plots through open-source research. This included access to court documents from many of the countries in the database. Moreover, we conducted forty interviews with police investigators, family members and friends of attackers, lawyers and other individuals close to the cases.[19]

The authors considered that studying thwarted attacks, which are frequently overlooked and rarely paired with successful attacks in the literature, offered new variables to explore and produced valuable quantitative insights on whether the way in which an individual becomes radicalised affects the kind of actions they end up committing. The authors acknowledge that many thwarted attacks never become publicly known. Thus the database contains an extensive, but likely non-exhaustive, sampling of plots where public information was made available.

Based on a preliminary study of the database, the authors identified five categories that broadly encompassed how perpetrators became radicalised. These are “mostly offline”, “mostly online”, “both”, “online asocial radicalisation” and “unknown”. The definitions are provided in the table below:

CATEGORIES	CRITERIA AND DEFINITION
Mostly offline	The individual appeared to have been radicalised outside the online world, in contact with siblings, relatives, friends, recruiters or like-minded individuals in mosques, prisons or other offline settings.
Mostly online	The individual appeared to have been radicalised in the online world, in contact with like-minded individuals on apps such as Telegram and/or with the mentorship or guidance of a recruiter in an online setting.
Both	Both the offline and online world appeared to have played a significant role in radicalising the individual, as he/she had relevant offline and online connections that overlapped over time.
Online asocial radicalisation	The individual had no online or offline social connections and had seemingly been radicalised by exposure to propaganda on the Internet. Individuals were coded as being online asocially radicalised only when the respective authorities have publicly described them as such.
Unknown	There was not enough data available to determine how the individual became radicalised or information was contradictory.

18 “Operaciones policiales contra el terrorismo yihadista en España”, Seguridad Internacional, www.seguridadinternacional.es/?q=es/content/operaciones-policiales-contra-el-terrorismo-yihadista-en-espa%C3%B1#seccion22

19 3 police investigators, 13 family and friends, 6 lawyers, 18 individuals close to cases

In coding individuals into their categories of radicalisation, the authors sought information from official sources, such as government reports, court cases and media reports that quoted a public official (police, prosecutor, defence lawyer or minister) or a close family member or friend. In some cases, this information was supplemented with interviews with investigators of the cases and access to additional police reports and court transcripts. In the absence of official sources, the authors relied on long investigative media reports from reputable sources to reconstruct the timeline of an individual's radicalisation, particularly searching for potential markers (such as a radicalised sibling, prison time or social media activity) that would allow to categorise the individual into one of the five categories.

Information available in any media article was cross-referenced with at least two other sources to ensure the veracity of the claims. The authors consulted around 600 sources, primarily in English and French, with some articles in Spanish and German. Efforts have been made to ensure that there are no duplicates in the database. The information was recoded in several occasions to account for new court cases and sources. Even so, the researchers acknowledge that as new information comes to light, particularly as some of the later suspects make their way through the legal system, the coding decisions could be amended.

3 Findings

Figure 1 displays the type of actors in our database. Out of the 439 perpetrators in our database, 12% were minors at the time of their arrest/attack and 92% were men. Those who acted in groups (that is, of two or more individuals) made up 63% of those in the database. Actors who were radicalised mostly in offline settings (offliners) accounted for 54% of the database followed by 18% who were radicalised in mostly online settings (onliners).

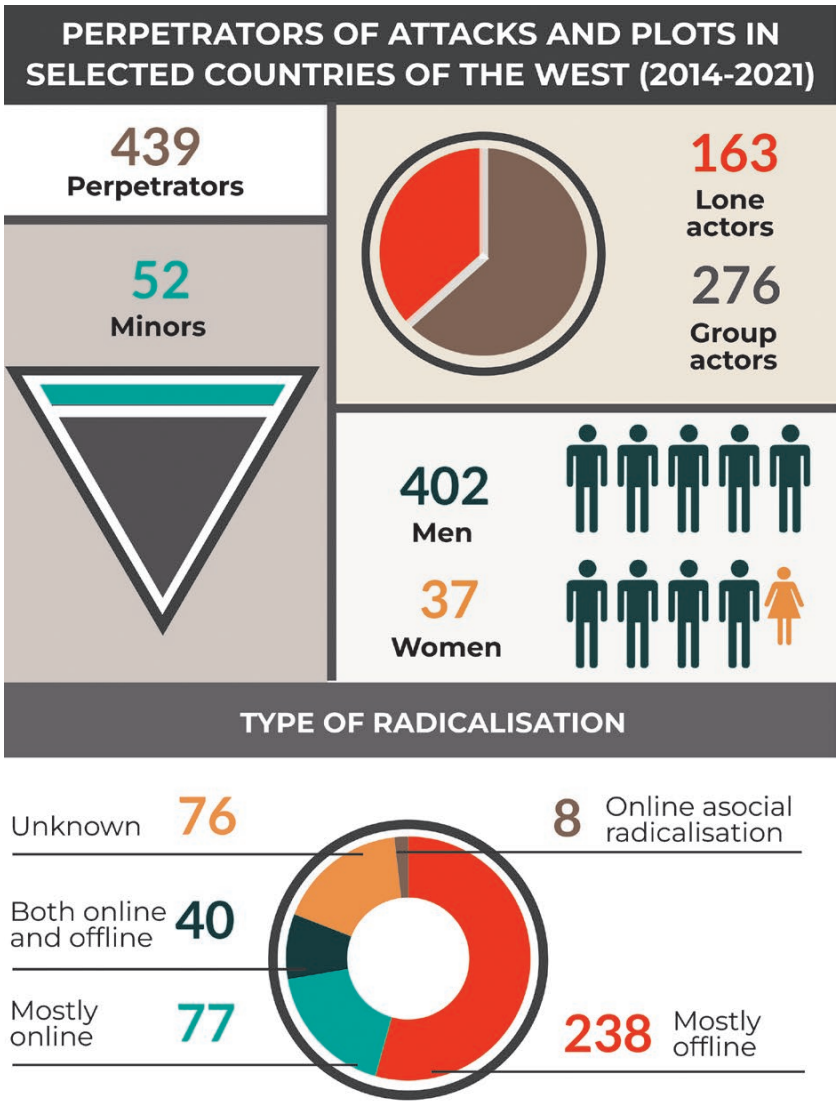

Figure 1. Perpetrators of completed and thwarted attacks

Figure 2 displays an overview of the type, location and frequency of attacks. The database contains 245 completed and thwarted attacks over seven years (1 January 2014 to 1 January 2021) in eight Western countries: Australia, Austria, Belgium, France, Germany, Spain, the United Kingdom and the United States. Out of the 245 attacks, 93 were completed and 152 were thwarted. We found 163 attacks to have been carried out by lone actors while 82 were carried out by groups.

The data shows fluctuations in the number of people involved in plots or attacks, with the peak taking place in 2016 and 2017. After the peak, there was a larger decline in group actors than lone actors in completed attacks.

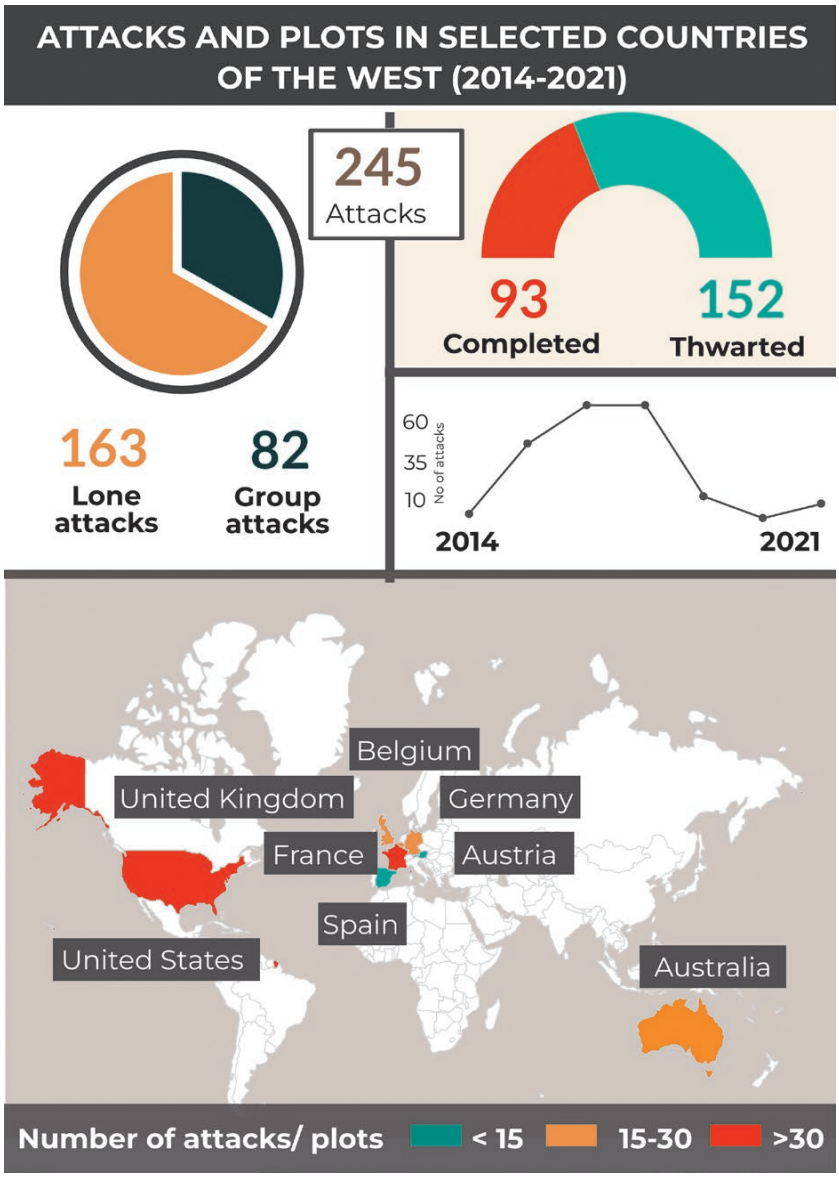

Figure 2. Attacks and plots in selected countries (2014–2021)

Who is More Likely to Complete an Attack?

Figure 3 shows that offliners are more likely to succeed in completing their attacks compared to other radicalisation setting types.

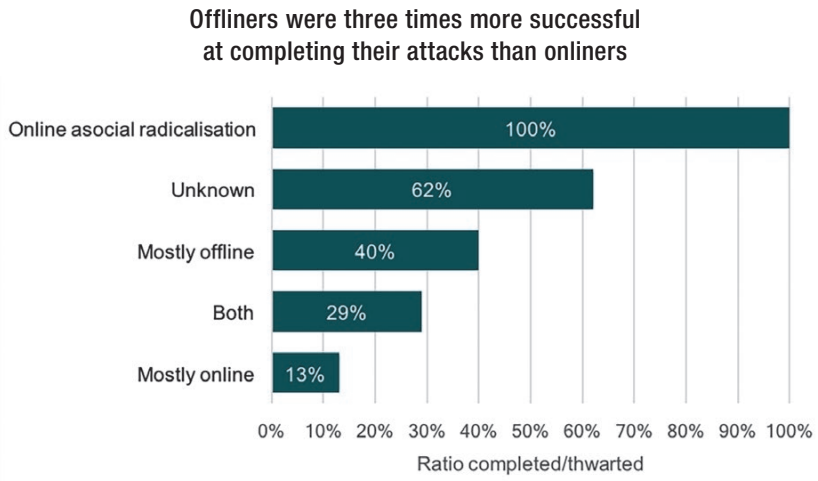

Figure 3. Offline vs online attack completion rate

Those who were radicalised mostly offline were nearly three times higher in their attack completion rate than those who were radicalised mostly online (40% vs 13%, respectively). Offliners showed a better than one in three rate of completing their attacks whereas onliners had a less than one in eight chance of completion, which was the lowest rate in the database. All categories had more attacks thwarted than completed with the exception of the eight people who were categorised as being asocially radicalised online, all of whom completed their attacks.

The database found that out of all the individuals involved in successful attacks, only 7% had been radicalised online, in contrast to the 55% who had been radicalised offline. When comparing the ratios of successful/thwarted attacks by online radicalised attackers (9:68) and those by offline radicalised attackers (68:170), the authors found that offliners are three times as successful.

Why are Onliners so Likely to Get Caught?

One plausible hypothesis as to why onliners are more likely to be thwarted compared to other groups is that perhaps their online activity, in particular their social activity, is what brings them to the attention of the police. Indeed, several onliners were apprehended because they sought out someone on social media to assist with their plots who turned out to be a police informant or an undercover agent.

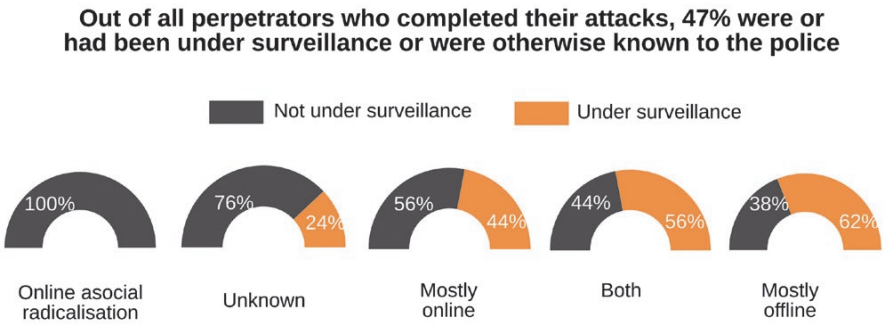

Figure 4. Percentage of attackers under surveillance

Some 47% of all individuals who committed successful attacks were or had been under police surveillance at some point or were known to counterterrorism police. Offliners were 1.5 times more likely than onliners to have been known to the police or under surveillance.

Who Caused the Most Injuries and Deaths?

A key issue for policy and practice is to know which radicalisation type led to the most violence. In particular, we are interested to know which attacks by the actors of various radicalisation types led to the most injured and dead. Figures 5 and 6 show that those radicalised in offline settings caused the most injuries and fatalities.

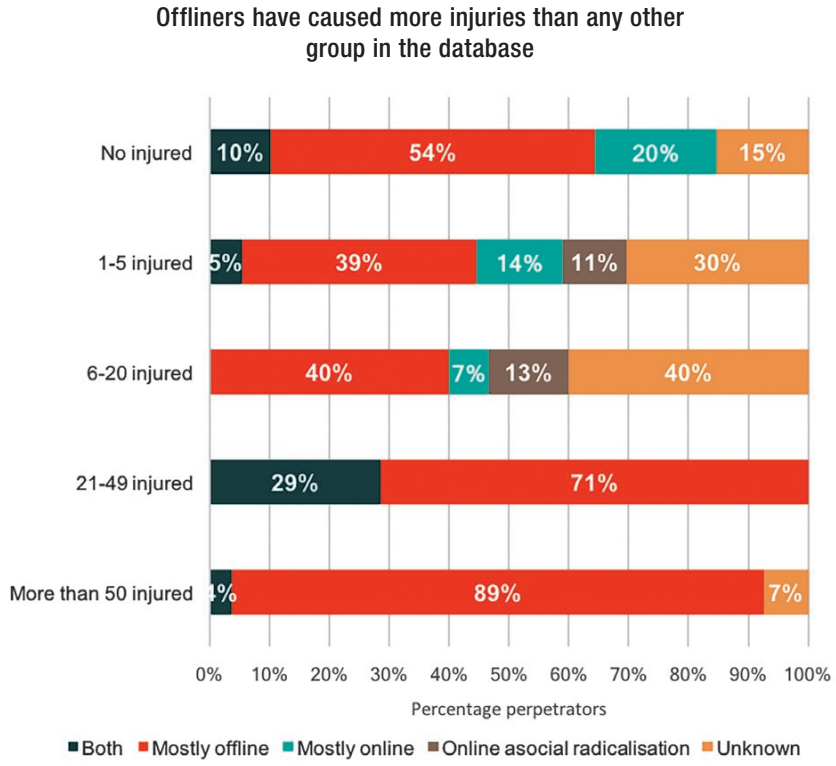

Figure 5. Attacker injury rate

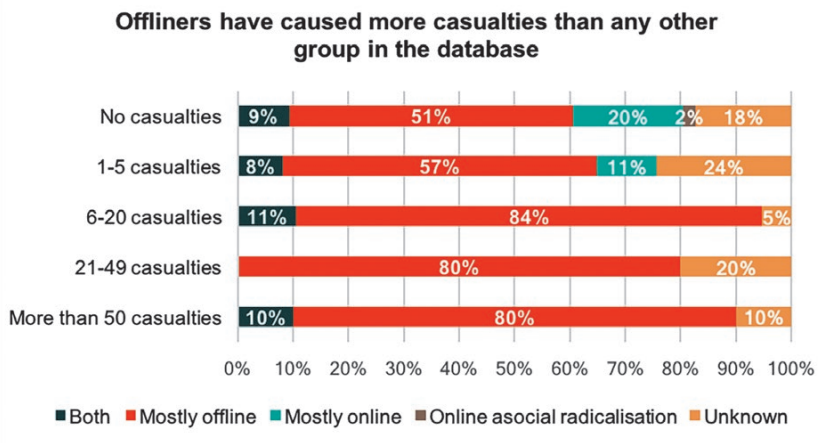

Figure 6. Attacker lethality rate

Those radicalised in offline settings caused more casualties than any other group in the database. They were 18 times more lethal than those radicalised in online settings. They were also 1.5 times more lethal than those coded as unknown and three times more than those coded as both. Online asocially radicalised individuals did not kill anyone. The total number of injuries and deaths by onliners who completed an attack is 30 and 7 respectively, whereas the total number of injuries and deaths by offliners is 1,780 and 370, respectively.

In the database, 16% of individuals (71 in total) carried out attacks (44 in total) that resulted in casualties. When we zoom into these 71 individuals, we find that 69% had been radicalised mostly offline while only 6% were radicalised mostly online, which is the smallest proportion in the database (8% were both, 17% unknown).

Figure 5 and 6 are broken down by impact rate, grouping the number of casualties and fatalities respectively.

Low impact: Some 52% were involved in attacks with one to five casualties, including the attacks in Normandy in 2016, Parramatta in 2015 and Hanover 2016. All categories of radicalisation were present in this tier.

Medium impact: Some 27% were involved in attacks with six to 20 casualties, including the attacks in Berlin in 2016, the Charlie Hebdo office in Paris in 2105, San Bernardino in 2015 and Barcelona in 2017. Most attackers had been radicalised offline, with some in the categories both and unknown.

High impact: Some 7% were involved in attacks with 21 to 49 casualties, including the attacks in Manchester in 2017, Brussels in 2016 and Florida in 2016. Most had been radicalised offline.

Very high impact: Some 14% were involved in attacks with more than fifty casualties, including the attacks in Nice in 2016 and Paris in 2015. Most assailants had been radicalised offline.

As can be seen in Figure 6, offliners have the highest number of casualties in all impact categories. This is expected, as there are more offliners in the database than any other category. However, onliners are only present in the low impact category (one to five casualties). This means that onliners not only have the lowest rate of success in completing an attack but are also the least lethal when they do succeed.

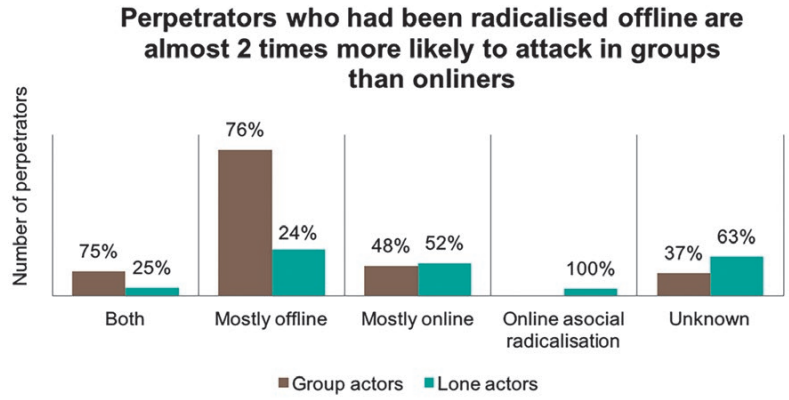

Figure 7. Lone vs group, online vs offline

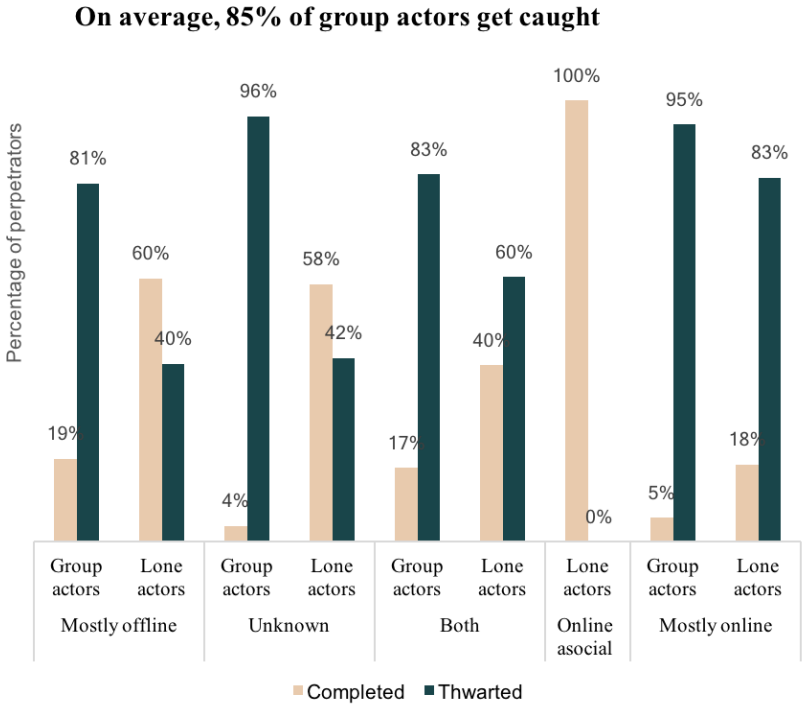

Figure 8. Group vs lone actor completion rate by radicalisation setting

Those who were radicalised mostly offline had a greater bias towards acting in groups. They were three times as likely to attack in groups than alone. Those who radicalised mostly online, conversely, had an even distribution between acting alone or in groups. Out of those who attacked in a group, 66% were offliners while only 13% were onliners.

When those radicalised mostly offline attack alone, they are much more likely to succeed in completing their attack (60% completed, 40% thwarted). When offliners attack in groups, however, they have only a 19% rate of completing an attack, with 81% of attacks thwarted. While those radicalised mostly online have a higher rate of being thwarted in general, they have three times the rate of completing an attack if they attacked alone versus in a group (5% vs 18%, respectively). Lone actor offliners completed an attack at three times the rate of lone actor onliners (60% vs 18%, respectively).

This means that those who were radicalised mostly offline and attacked alone are by far the most likely to succeed. Offliners who acted in groups were thwarted four times more than if they acted alone. Looking only at those attacks that were thwarted, 74% of them were group actors. However, offliners who attacked in groups had a 15% higher lethality rate than when they acted alone. Thus, from the terrorist perspective, groups are a double-edged sword: they pose the highest risk of getting caught by the authorities before the attack, but when they are able to carry out the attack, they are the deadliest.

Who are the Offliners Who Attack in Groups?

Perhaps one reason that offliners are more likely to act in groups is because they plot their attacks with family members, friends or romantic partners. We found that 87% of those with radicalised friends and 74% of those with radicalised relatives (offliners and both) plotted in groups. Offliners and those coded as "both online and offline" had the most known friends, family members and partners who were radicalised.

This reinforces studies in the literature suggesting that strong interpersonal dynamics, such as those present in family and friend relationships, can play a strong role in radicalisation. Family dynamics also played an important role in driving individuals to attack together, usually in pairs of siblings (as seen in the Charlie Hebdo attack in 2015, the Bataclan attack in 2015 and the Barcelona attack in 2017, which brought together three sets of siblings).

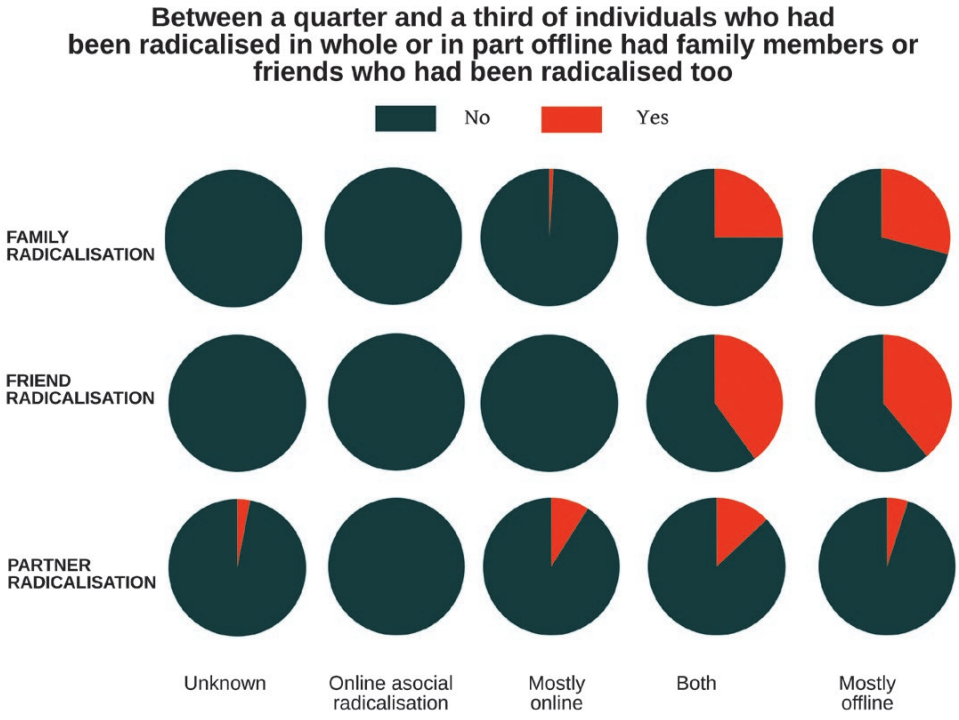

Figure 9. Family and friends radicalisation connection

Does a Criminal History Impact Outcomes?

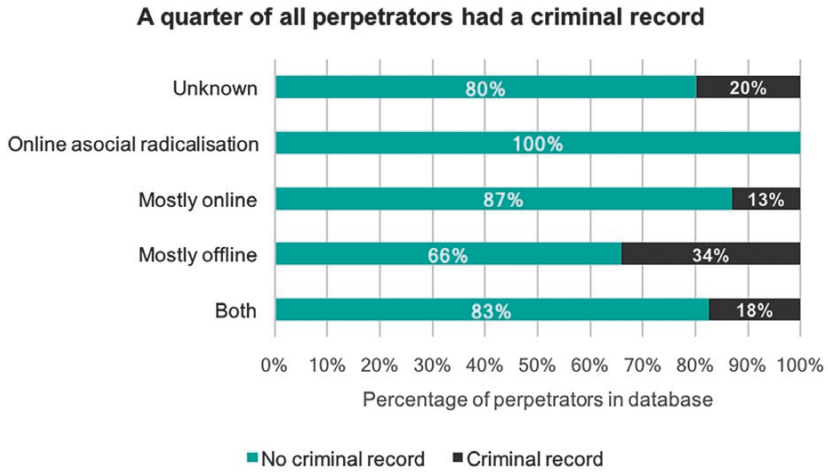

Figure 10. Criminal records and type of radicalisation

Previous research has discovered a crime-terror nexus with some analyses finding anywhere from a half to two thirds of Western FTFs possess a history of criminality. In this database, 26% of individuals had a criminal record, in some cases spanning long periods of time. The most common offences were petty crime, robbery, assault and drug-related crimes. This is considerably lower than findings on FTFs. It seems that those who seek to carry out a domestic act of terrorism are much less likely to possess a criminal background.

Figure 10 shows that those who were radicalised offline had the highest incidence of criminal backgrounds. Looking only at those who had a criminal record, more than 72% had been radicalised offline versus only 9% who had been radicalised online. Offliners included nearly three times as many people with a criminal record as onliners (34% vs 13%, respectively).

Does a History of Foreign Fighting Impact Outcomes?

Some 66 individuals in the database (15%) became foreign fighters and joined IS in Iraq and Syria or trained in other locations. An additional 12% attempted to become foreign fighters but were actively prevented from doing so (they were either arrested or had their passport revoked before travel), while a further 15% explicitly expressed a desire to travel to Syria but resorted to planning an attack instead.

Among those who became FTFs, Syria and Iraq under IS control were the most popular locations (85% of foreign fighters), followed by Afghanistan, Yemen, Libya and Somalia. The majority of foreign fighters were radicalised mostly offline (77%), with friend or family dynamics playing a significant role in 45% of cases. By contrast, 35% of non-foreign fighters had radicalised friends or relatives.

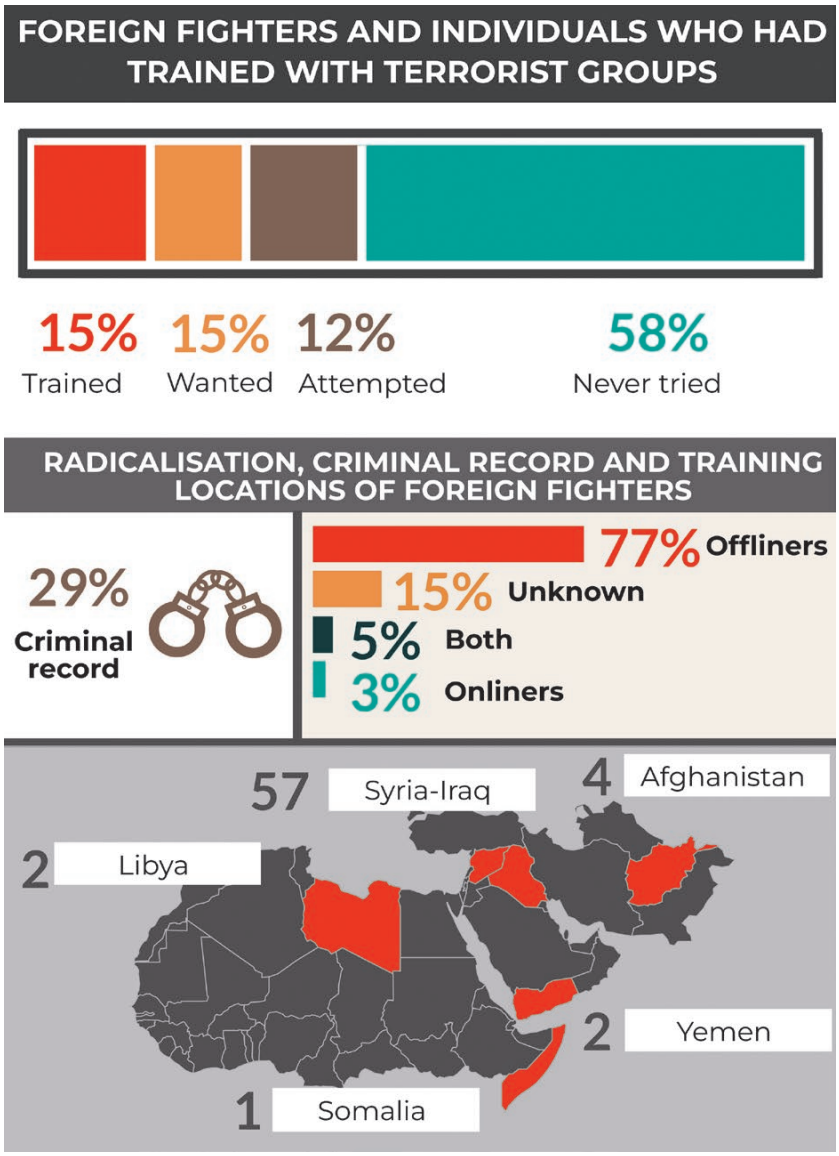

Figure 11. Foreign fighters and criminal records

Of the foreign fighters in the database, 73% attacked or plotted in groups, while 27% did so individually.

Some 29% of foreign fighters had a criminal record before training in terrorist locations. The most common offences were petty crime, robbery and violence. This criminal history percentage among foreign fighters who returned to carry out an attack is lower than the percentage found in Western foreign fighters in general. Basra and Neumann found that half of the foreign fighters from several Western countries (including those who did not participate in plots or attacks at home) had a criminal record before joining a terrorist group in a foreign land.

Did Length of Training Increase the Likelihood of Foreign Fighters Carrying Out Attacks?

In 2016, Nesser, Stenersen and Oftedal argued that the inclusion of foreign fighters in plots increased the risk of detection because they were more likely to come to the police's attention. However, this database found that foreign fighters are no more likely to be involved in thwarted attacks than non-foreign fighters. Foreign fighters have almost the same completion rate as non-foreign fighters (29% vs 28%).

The case of Mohamed Ouharani, who attempted to commit a gun attack against Shia in Créteil, France, is illustrative in this regard. Ouharani was not arrested right after returning from Syria, but rather after conducting several searches on the Internet, including into different weapons and Mehdi Nemmouche's attack at the Jewish Museum in Belgium. It was his online rather than offline activity that led to him being caught.

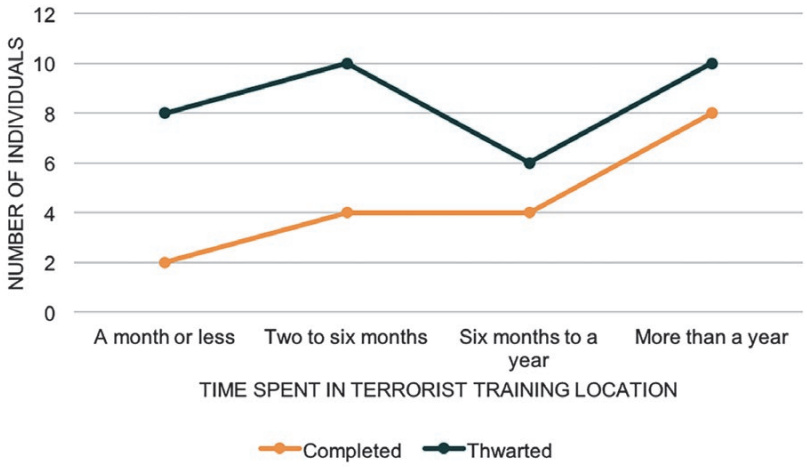

Figure 12. Length of time spent as a foreign fighter and attack completion rate

According to the database, the success rate also increased the longer individuals stayed in training camps, suggesting that they had received more effective training on how to evade counterterrorism forces. If they spent less than a month in a terrorist training location, they had a 25% rate of completing an attack without getting thwarted. But if they spent more than a year in a training location, they had an 80% rate of completing an attack without getting thwarted. That means their success to failure ratio more than tripled if they spent more than a year at a training location.

Some 63% of all of foreign fighters involved in successful plots had spent more than six months training in Syria: a significant proportion (42%) of all foreign fighters stayed for more than a year. Those who spent more than six months training were twice as likely as those who spent less than six months to succeed in their attack (63% vs 32%).

These results do not imply that staying for a prolonged period of time training abroad was an effective way to avoid detection by counterterrorism police, as 56% of those who trained in terrorist training camps for more than a year were caught; in fact, across the board, more were thwarted than successful, regardless of time spent in training camps.

Are Young People More Likely to be Radicalised Online?

Most individuals in the database were radicalised offline, but the trend is changing for younger generations, who are more likely to have been radicalised online than older generations

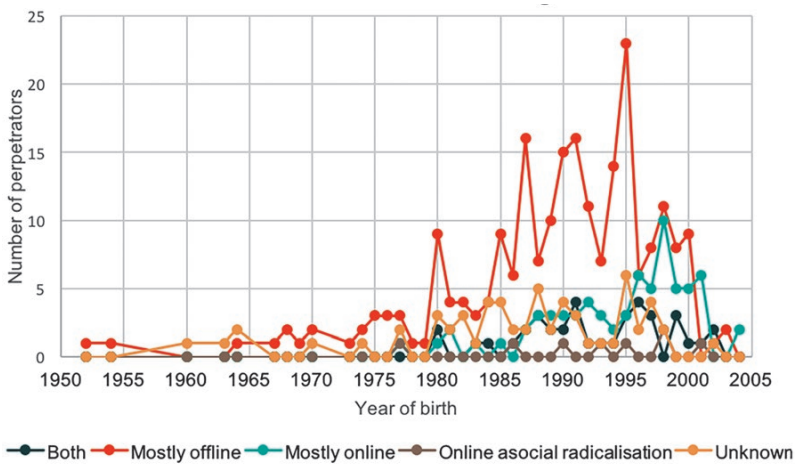

Figure 13. Age and type of radicalisation

Perhaps the difference in those radicalised offline versus online can be explained by age, in that younger people may have been radicalised more online than offline. Figure 13 maps the known years of birth of individuals in the database with their radicalisation setting. Those born in the mid-1980s to mid-1990s had the highest incidence of offline radicalisation. We see an increase in online radicalisation for those born after the mid-1990s but it stays on a par with the rate of offline radicalisation.

In the database, 12% were minors at the time of their attack or arrest. We found that 38% of minors had been radicalised online compared to 15% of adults. While the rate of online radicalisation is higher in minors than adults, the majority of minors was still radicalised offline or both online and offline. Half of all minors who were radicalised offline were recruited by a family member. This demonstrates the importance of family environments when preventing youth radicalisation.

Are Women More Likely to Radicalise Online?

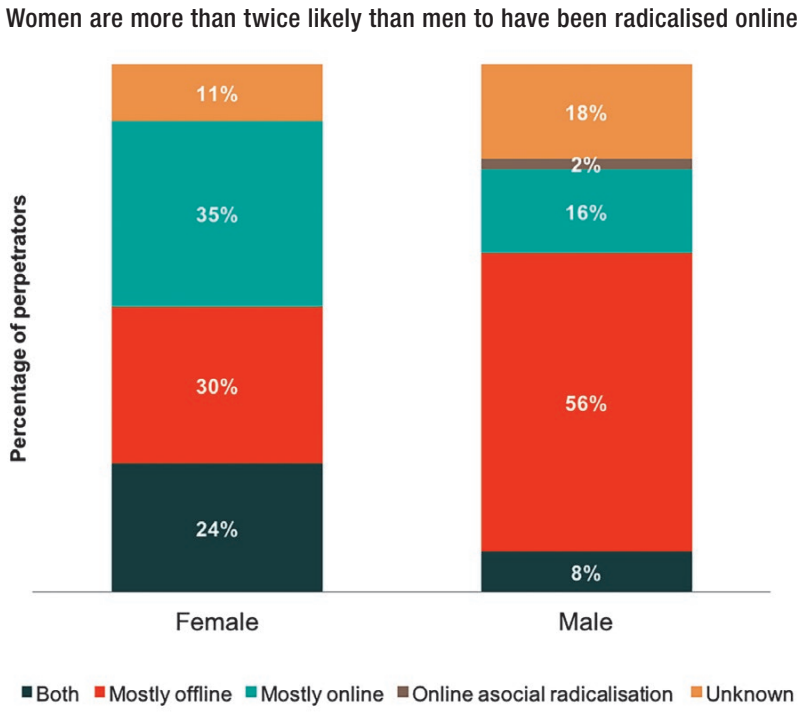

Figure 14. Gender and radicalisation type

In the database, 8% of the perpetrators are women (37). Women are 15% more likely to have been radicalised online than offline. Women are also more than 2 times as likely to have been radicalised online than men; 35% of women underwent this type of radicalisation versus only 16% of men. Onliners, which women are more likely to be, were almost twice as likely to have been radicalised with their partners than offliners. There were several cases in the database where a couple had met and been radicalised together online. Women in the database were 3.5 times more likely to be minors than men (35% vs 10%). Women were more likely to be involved in groups than attack alone (86%). Women were less successful than men in their attacks (10% vs 30%).

Why this Gender Effect?

This database echoes the findings in the literature that women tend to be more likely to be radicalised online. Research by the Tony Blair Institute for Global Change focusing on UK jihadists found that 44% of their sample of women had been partly radicalised online, with half having had no offline influence, while only 4% of the men had an online element in their radicalisation. Pearson and Winterbotham's empirical research found that "online social networks appeared to be the primary location of female radicalisation" with the caveat that "where women had access to public spaces, and were not subjected

to cultural restrictions, they could be recruited offline via the same mechanisms as young men".[20]

It should be noted that the total sample of women (37) was much smaller in number than the total sample of men (402). Nonetheless, the difference in sampling also corresponds to historical research about women's involvement in terrorism showing that women have tended to adopt more supportive roles in terrorism, although past and recent literature has also highlighted the active involvement of women in attacks, such as Boko Haram's unprecedented use of women as suicide bombers and IS's shift to using women in combat.

How was Social Media Used?

Another issue of interest for policy and practice is to understand how social media is used by terrorists. We found that at least 39% of individuals in the database regularly used social media and apps to communicate with, plot with and radicalise like-minded individuals. There were three main categories of use to which social media and apps were put: radicalisation (49%), operations or communication (28%) and posting (23%).

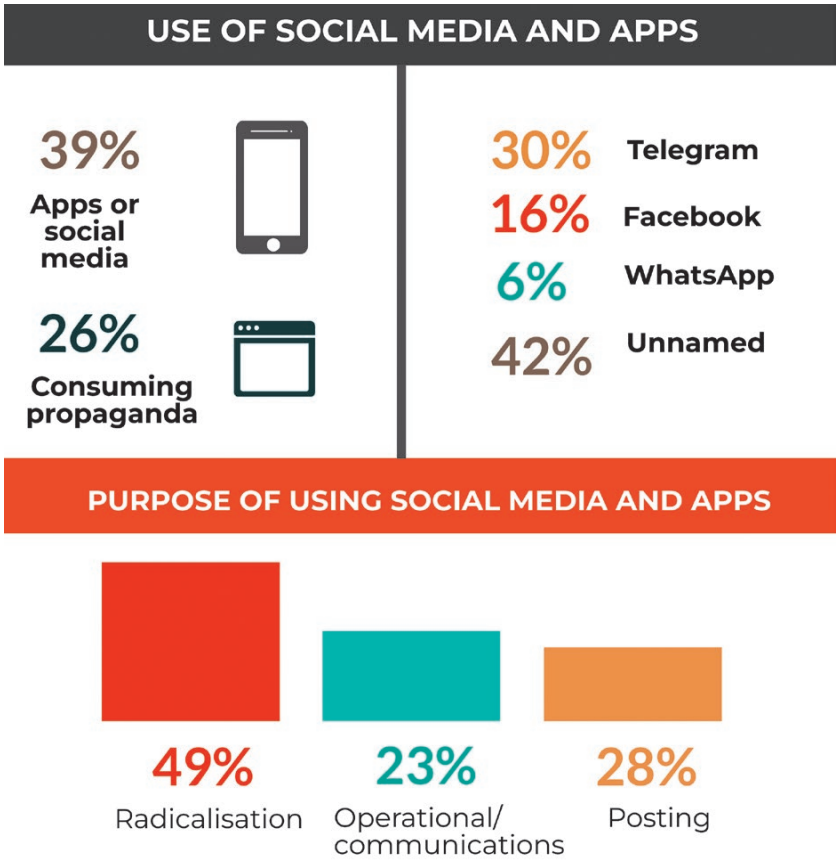

Figure 15. Social media platform use

20 Elizabeth Pearson and Emily Winterbotham, "Women, Gender and Daesh Radicalisation", The RUSI Journal, 162:3, 60-72, https://f-origin.hypotheses.org/wp-content/blogs.dir/2725/files/2017/08/Women-Gender-and-Daesh-Radicalisation.pdf

From this sample of users of social media, at least 35% posted about their extreme ideas on social media before succeeding in committing an attack. Where platforms were named, the most popular platforms were Telegram (30%), Facebook (16%) and WhatsApp (6%). At least another 23% were using undisclosed encrypted communications apps and another 17% of individuals were active on other social platforms (not named). At least 26% were consuming propaganda. Most of this propaganda was ideological (23%, with multiple references to al-Qaeda ideologue Anwar al-Awlaki as inspiration), followed by operational manuals (at least 15%).

4 Conclusion

This report explored the differences in trajectories between those who were radicalised primarily offline versus those who were radicalised primarily online in terms of their jihadist-linked plots and attacks in the West. The findings suggest that the major threat comes from those being radicalised in mostly offline settings, who are largely those being radicalised by groups of friends or family. Offliners are more likely to be placed on watchlists than those mostly radicalised online and yet are still better able to slip through the net than their online counterparts. They are more likely to succeed when they do plot an attack and they are far more lethal than those radicalised mostly online. We found that offline radicalisation is still the primary setting for those who engage in or attempt to engage in acts of terrorism. However, we do see an increase in online radicalisation among young people and women. It is yet to be determined if this trend will cause online radicalisation to surpass offline radicalisation among these cohorts. Our evidence suggests that while online radicalisation does exist and is a problem, it is not the primary problem and not the most pertinent for security. The threat is still largely in the offline space and almost certainly requires offline solutions.

Such solutions can involve reducing bystander effects whereby those who are close to a violent actor (e.g. friend, family, co-worker, neighbour, etc.) do not report them to the police despite being aware of an impending attack.[21] Research in the US[22] and UK[23] has indicated that improving relations between police and community members could help reduce this effect. The process of how to improve these relationships can be found in research on regular policing such as in Australia where they created community liaison teams that did not seek to elicit information directly about illicit activity but rather listened to local grievances and helped them improve those conditions.[24]

Other options that blend offline and online activities can include things like ideological inoculation whereby mild forms of an extremist group's ideas can be presented to individuals in a space (online or offline) where they can argue against them and come to firm (negative) conclusions about the ideology.[25] Other programmatic efforts include norm-change interventions which, often through media, convince target populations that their broader-peer group does not support certain extremist values or behaviours. These efforts have been particularly successful in post-conflict reconciliation

21 Paul Gill, John Horgan and Paige Deckert, 'Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists', *Journal of Forensic Sciences* (Vol. 59, No. 2, 2014), pp. 425–35.
22 Michael J Williams, John G Horgan and William P Evans, 'The Critical Role of Friends in Networks for Countering Violent Extremism: Toward a Theory of Vicarious Help-Seeking', *Behavioral Sciences of Terrorism and Political Aggression* (Vol. 8, No. 1, 2016), pp. 45–65.
23 Rachel Briggs, 'Community Engagement for Counterterrorism: Lessons from the United Kingdom', *International Affairs* (Vol. 86, No. 4, 2010), pp. 971–81;
24 Adrian Cherney and Kristina Murphy, 'Police and community cooperation in counterterrorism: Evidence and insights from Australia', *Studies in Conflict & Terrorism* (Vol. 40, No.12, 2017), pp. 1023-1037.
25 Kurt Braddock, 'Vaccinating Against Hate: Using Attitudinal Inoculation to Confer Resistance to Persuasion by Extremist Propaganda', *Terrorism and Political Violence*, 25 November 2019.

environments such as in Rwanda[26] and the DRC[27] but also have been shown to work on jihadist supporters.[28] Yet another option is that of counter-engagement, rather than just counter-messaging, where activities online and offline can help engage susceptible individuals into groups that provide belonging, purpose, and any other factors that extremists might exploit if lacking in an individual.[29]

Other studies have investigated the use of social media by extremists such as the START PRIUS dataset analysis.[30] The START study focused solely on US based extremists between 2005 and 2016 and included both violent and non-violent extremist from Islamist, far-left, far-right and single-issue movements/causes. The study found that while social media use had exponentially increased over those years, many would-be foreign fighters and terrorist were caught due to their use of those platforms. These results coincide with our findings that social interaction online helped authorities intervene before an attack could unfold.

The START study also found that between 2011 and 2016, 16.9% of extremists in their database were primarily radicalised online. This is very close to our finding of 18% being mostly radicalised online. However, when they looked only at the subset of individuals who completed or were planning an attack (226 individuals in total), 52.22% of them had been radicalised online. This number is almost three times as many as we found. It is not clear why this difference exists but perhaps there is large variation from country to country and between extremist movements which underlines the importance of contextually tailored approaches to preventing terrorist attacks and radicalisation.

The START study did find that the most successful attackers in their database were those who abstained from using social media altogether. This coincides with our findings that offliners were the most successful attackers and especially those that avoided online social activity previous to carrying out an attack to evade detection by police.

In addition to providing answers regarding the outcomes of those radicalised offline versus online, this report contributes in another significant way to the terrorism and radicalisation literature. It builds upon and combines existing databases to create a new large-scale database consisting of 439 perpetrators in 245 thwarted and completed jihadist-linked attack over seven years in eight Western countries. The granularity of the data combined over a timescale and geography allows for a robust quantitative analysis. The database itself contributes to a field where the evidence base is still growing.

26 Elizabeth Levy Paluck, 'Reducing Intergroup Prejudice and Conflict Using the Media: A Field Experiment in Rwanda', *Journal of Personality and Social Psychology* (Vol. 96, No. 3, 2009), pp. 574–87.
27 Elizabeth Levy Paluck, 'Is It Better Not to Talk? Group Polarization, Extended Contact, and Perspective Taking in Eastern Democratic Republic of Congo', *Personality and Social Psychology Bulletin* (Vol. 36, No. 9, 2010), pp. 1170–85.
28 Nafees Hamid et al., 'Neuroimaging "Will to Fight" For Sacred Values: An Empirical Case Study with Supporters of an Al Qaeda Associate', *Royal Society Open Science*, 12 June 2019.
29 Nafees Hamid, 'Don't Just Counter-Message; Counter-Engage', International Centre for Counter-Terrorism, 28 November 2018, <https://icct.nl/publication/dont-just-counter-message-counter-engage/>, accessed 28 January 2020.
30 Jensen, Michael, P. James, G. Lafree, A. Safer-Lichtenstein, and E. Yates. "The use of social media by United States extremists." *START, CollegePark* (2018). https://www.start.umd.edu/pubs/START_PIRUS_UseOfSocialMediaByUSExtremists_ResearchBrief_July2018.pdf

However, the generalisability of our results is limited by the fact that we focused only on jihadist-linked attacks and plots, and only in Western countries. We encourage other researchers to build similar databases for other violent movements and in non-Western countries. Such databases can then be combined to look for broader trends across the world.

It should also be pointed out that radicalisation processes and terrorism tactics are dynamic systems that change constantly as a result of counter-measures. Continued research in the style presented here can reveal how movements are adapting to counter-measures by governments and social media companies. Insights from this kind of research can reveal whether such measures are effective, counter-productive, or simply altering the tactics being used by violent extremist movements. In some cases, this may help the public and private sectors to stay one-step ahead of those who orchestrate or inspire acts of political violence.

Policy Section

This policy section has been written by Inga Kristina Trauthig, Research Fellow, and Amarnath Amarasingam, Senior Research Fellow, at the International Centre for the Study of Radicalisation (ICSR) at King's College London. It provides policy recommendations and is produced independently by ICSR. Recommendations do not necessarily represent the views of the report authors.

The key findings of this report carry corresponding policy implications for governments around the world as the quantitative analysis of this report implies a prioritisation of counter-programmes that focus on or at least include the offline space. At the same time, technology companies are well aware that they are facing challenges with regard to continuous exploitation of the online space by terrorists, such as disseminating propaganda. The following section seeks to achieve a threefold aim: first, to deliver concrete policy recommendations for governmental stakeholders; second, to outline policy options and strategic foresight for technology companies; and, finally, in hand with [1] and [2], to serve as a reference point for a future evaluation of tech policies in order to assess dos and don'ts of technology legislation around the globe.

With this, the policy section ensures that the Global Network on Extremism and Technology (GNET), the academic research arm of the Global Internet Forum to Counter Terrorism (GIFCT), is academically advising and supporting technology companies and policymakers on how to better understand the ways in which terrorists are using information technology. This is designed to fulfil not only GIFCT's pillar of learning, but ultimately to improve prevention and responses to terrorist and violent extremist attacks.

1. Focus: Policymakers

The analysed lethality of (potential) terrorist attackers radicalised either offline or online (or both) raises relevant points that should be addressed and factored in by governmental stakeholders in charge of keeping their societies safe. In addition to national governments, international (EU, UN, and so on) policymakers, especially security policymakers and stakeholders working on prevention programmes, should take note and consider the effectiveness of individual actors radicalised offline for their policymaking.

- As this report has outlined, groups, regardless of the radicalisation setting, achieved a significantly lower completion rate and lone attackers radicalised offline are associated with the highest success rates. This carries consequences for law enforcement officials: while they are clearly adept at monitoring and infiltrating groups, lone actors still remain a problem. The lethality of lone actors reinforces the concern that these types of attacks will continue to threaten the population and counterterrorism practices might need to adapt further.

- The most significant takeaway from the analysis conducted in this report is that the investment of massive amounts of resources to counter the online threat should not lose sight of what is happening offline: “offliners” conduct more lethal attacks, according to the report’s findings. Therefore, local, national and international policymakers should continue to invest in local prevention efforts and initiatives and recognize that there are no blanket technological solutions for all terrorist attacks.

- In line with this call for continued efforts directed at offline counterterrorism and counter-violent extremism (CVE) programmes, the report also highlights the importance of targeted programmes. For example, the rate of individuals radicalised online increases significantly when looking at younger age groups (including minors). Attempts at devising online programmes, such as counter-messaging campaigns, might therefore benefit significantly by having an age group in mind during their design. Similarly, the report shows the higher importance of the online space for female radicalisation compared to male radicalisation (albeit female radicalisation represents only a small proportion of the database overall).

- Finally, the above points outline a well-known characteristic of radicalisation processes, namely their complexity. Government stakeholders are therefore well advised to continue working with civil society stakeholders from diverse backgrounds while acknowledging the need to have those actors operate with a certain degree of flexibility and freedom in order to reach some individuals or groups.

2. Focus: Technology Companies

In addition to the report findings and their implications for governmental stakeholders, the analysis is also relevant for technology companies aiming to rein in the exploitation of their platforms for malevolent purposes, such as recruitment into terrorist groups.

- The main finding of the report, that pure online radicalisation seems to result in fewer or less lethal attacks than had been suggested with the rise of IS and the foreign terrorist fighter phenomenon, is a welcome insight. However, it is clear that tech companies need to continue to work towards safer online spaces, as almost 40% of individuals in the report’s database regularly used social media and apps to plot, communicate with, and radicalise like-minded individuals. In other words, while purely online radicalization, according to the findings of this study, often lead to less lethal attacks, that is not the only measure that is significant.

- Similar to the point made in the previous section, the fact that minors were almost three times more likely to have radicalised online should be taken to heart by technology companies. For instance, existing co-operation with other stakeholders (such as civil society groups and/or governments) could be further enhanced by designing different efforts for different age groups and genders.

- The report does not address cross-platform migration and communication per se but traces the social media engagement of different (potential) terrorists by noting that when platforms

were named, the most popular platforms were Telegram (30%), Facebook (16%) and WhatsApp (6%), with at least another 23% using undisclosed encrypted communications apps and another 17% active on unnamed social platforms. This suggests two possible points of action for technology companies: first, the need for continued co-operation between companies and, second, an honest discussion about the use of encrypted communication apps by extremists.

3. Focus: Strategic Foresight and Broader Implications

In addition to the policy recommendations derived directly from the above report, broader implications and strategic deliberations are also evident from this study of the differences in outcomes for those who have been primarily radicalised offline versus online.

- Since this GNET report focused on jihadist-inspired successful and thwarted attacks, the most pressing big picture question is how the results of this study would compare to similar datasets focusing on, for example, right-wing extremism. For instance, the relevance of alternative social media platforms or the opportunities of the decentralised web have been exploited by right-wing groups already, but the importance of these compared to offline factors of radicalisation and/or more traditional social media platforms is underexplored.

- Broadly speaking, assessing technological developments, such as the metaverse and its impact (or non-impact) on radicalisation, would be important. Policies related to extremism are often reactive, as the current landscape is fast-moving and eclectic. While social media companies can learn from past challenges, such as the rise of the Islamic State's online presence from 2012 onwards, there is a real need to think outside the box when it comes to the current threat.

Global Network
on Extremism & Technology

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.