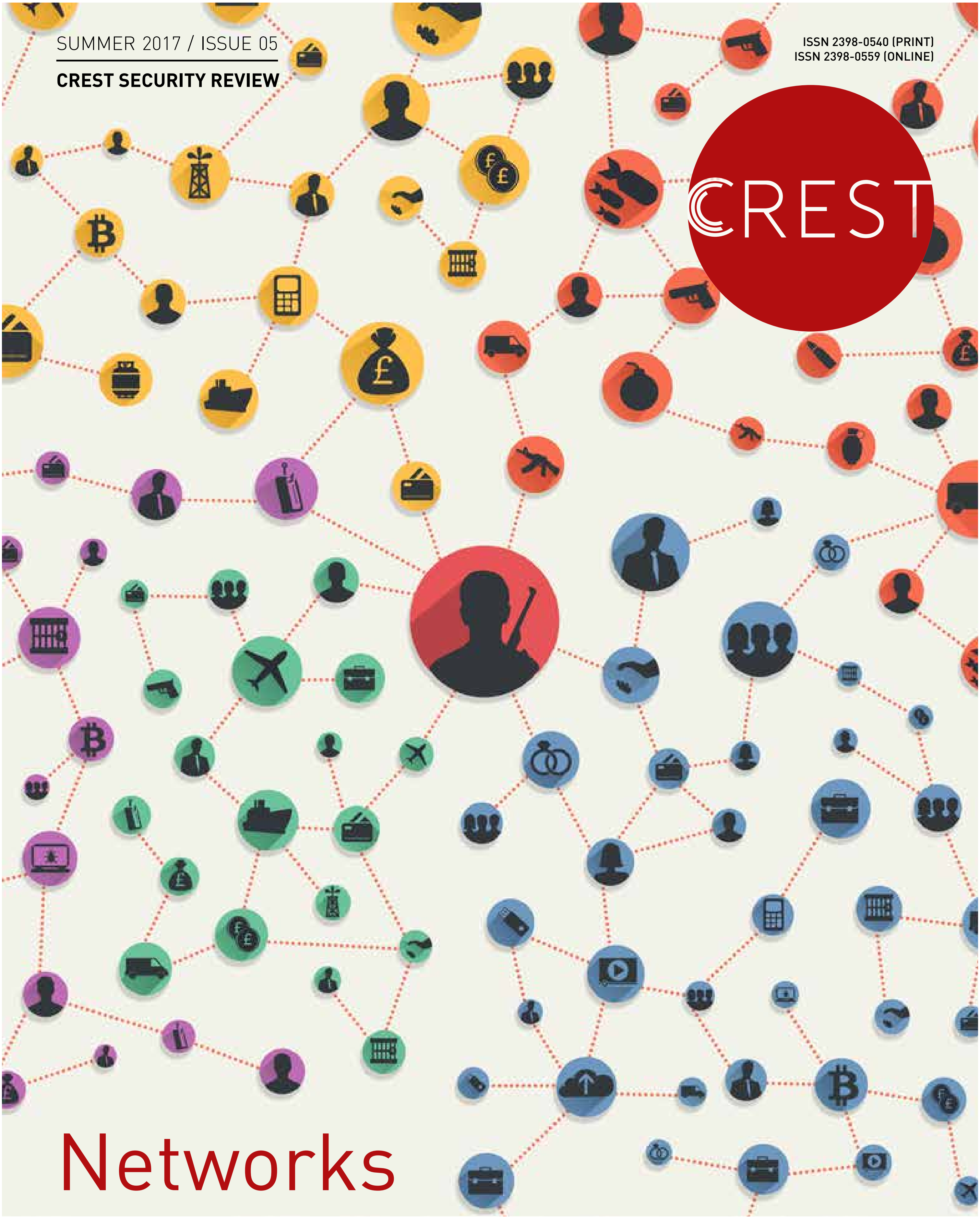
SUMMER 2017 / ISSUE 05

CREST SECURITY REVIEW

ISSN 2398-0540 (PRINT)
ISSN 2398-0559 (ONLINE)



Networks

NETWORKS AND THEIR IMPLICATIONS FOR SECURITY PRACTITIONERS – p4

PREDICTING THE IMPACT OF BAD APPLES ON TEAM PERFORMANCE – p8

HOW ISLAMIC STATE USES TELEGRAM TO COMMUNICATE – p14

CONTENTS

NETWORKS

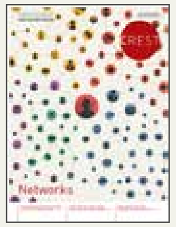
Highlights

KIM KARDASHIAN AND COMPLEX SYSTEMS

Can we predict and prepare for a co-ordinated event disrupting a complex system? – p10

BLUFFERS GUIDE TO NETWORKS

Don't know your betweenness centrality from your boundary spanner? Read our guide – p30



CREST SECURITY REVIEW
Editor – Matthew Francis
Guest Editor – Adam Joinson
Illustrator – Becky Stevens
Designer – Steve Longdale

To contact *CREST Security Review* please email
csr@crestresearch.ac.uk

FROM THE EDITOR

Networks matter. We learn how to connect with people around us through family networks, travel to work on transport networks, spend our pay through financial networks, often with people in our social networks.

Studying networks not only gives us an insight into our human behaviour. It also helps us understand weak points in critical networks, be it food or energy supply, or in the way a company is run.

> "Power does not reside in institutions, not even the state or large corporations. It is located in the networks that structure society."
>
> Manuel Castells, 2004,
> *Afterword: Why networks matter*

When focused on security threats, examining networks can highlight weak points in terrorist activities or vulnerabilities in our own defences.

When we decided to do an issue on networks, I was worried that we'd have a magazine full of blobs and lines! However, our Guest Editor for this issue, Adam Joinson, has done a sterling job putting together a bluffer's guide to network analysis. If you're new to this topic, then turn to page 30 and find out what those network diagrams mean. Adam and one of his Doctoral Researchers, Brittany Davidson, have also outlined why we should study networks, and how doing so can provide critical insights for security practitioners (p.4).

Turning to how studying networks can help us understand security threats, Martin Everett presents an analysis of covert networks, based on the Provisional IRA, on page 16. Dorothy Carter and Cynthia Maupin highlight the security implications of leadership networks (p.6) and Thilo Gross discusses how epidemics spread on networks (p.12).

Looking at one particular social network, Mia Bloom shows us how Islamic State use the messaging service, Telegram (p.14).

> Understanding weak points in networks can be useful in both offensive and defensive applications.

Using his research on the ties between team members, Jeroen de Jong demonstrates how we can predict the impact of 'bad apples' on team performance. On a similar theme, Rosalind Searle and Charis Rice look at how trust within large organisations can be maintained, even at times of upheaval.

In each issue of *CREST Security Review*, we also feature articles outside of our special focus. In this issue I am delighted to feature research on community reporting of potential terrorist threats.

Building on an earlier study in Australia by Michele Grossman, she and Paul Thomas have been funded by CREST to replicate the study in the UK. Their article presents some early findings on how people feel about reporting on their friends or family members. We also feature an introduction to the far-right landscape by Benjamin Lee (p.28), and provide you with details on how you can download a CREST Guide by Benjamin on this subject.

Please get in touch to tell me what you liked (or didn't) about this issue, and what you would like to see featured in the future. You can email me at m.d.francis@lancaster.ac.uk or contact me through the CREST website www.crestresearch.ac.uk

Matthew Francis
Editor, *CSR*

ADAM JOINSON AND BRITTANY DAVIDSON

WHY NETWORKS MATTER

What are networks?

Human organisation has always involved a structure of some form or other. In the workplace we have hierarchies and processes that formalise both responsibilities and the process of work. Who we report to, and our own line management responsibilities, are usually explicitly recorded, but not who we spend lunch time with, bounce ideas off, dislike, or collaborate on a project with. Across an entire organisation, often it is the hidden actions and interactions that lead to the successful completion of a task, and generate value.

The point of studying networks (in particular, but not just, social networks) is to reveal not only the hidden structure of these interactions, but how that structure influences everything from competitive advantage, resilience to outside interference, the spread of ideas and illnesses, and how ideas and practises move across a population. While many security practitioners will be well versed in link analysis, network analysis provides ways to study the structure of a network mathematically, and from that to identify novel insights into its likely resilience, hidden elements or how quickly information will spread across it.

The foundation of network science can be traced to mathematician Euler's 'The Solution of a Problem Relating to the Geometry of Position' in 1736, also known as the Seven Bridges of Königsberg. The crux of the problem was to find a walking route around the town where you cross each bridge only once – something that Euler identified as impossible.

But, what actually is a network?

A network is anything with two or more entities that are connected in some way or other. Typically, the entities are called 'nodes', and the connections 'edges'. In social network analysis, nodes are people, and edges ties between them (which can be kinship, communications or any other connection). These edges can have weights, which can be used to represent strength of relationships or amount of information flow. More widely, network science has been used to investigate the relationship between a large range of objects, including organisational and state-level alliances, biological eco-systems and the spread of pandemics in a population. We can understand and describe atoms and atomic structure in terms of their network, as well as understanding how this network structure may change (e.g., when a substance changes from a solid to a liquid state). There are also social networks (online and offline), biological and ecological networks (e.g., fungal networks), and more recently, we have technological, informational (e.g., internet, world wide web) and infrastructural networks (e.g., railway systems, power grids).

Implications for security practitioners

Understanding networks provides critical insights for security practitioners. For instance, al-Qaeda (AQ) has always been seen as adopting a networked organisation, with the leadership acting primarily as a focus for the dissemination of communications rather than providing a direct command and control function. This has made AQ highly resilient to outside interference, even when leadership members are disrupted. Meanwhile, Islamic State (IS) has tended to adopt a more traditional hierarchical command structure that reflected its territorial and governance ambitions. Understanding how groups are structured not only provides intelligence on possible connections, but also provides an insight as to the likely resilience of a group in the face of disruption. For instance, a difficult to detect cell might have members with weak connections to each other, with perhaps a single member acting as the 'bridge' to other groups. Suicide bombers and others most likely to be identified or caught tend to be kept on the periphery of terrorist groups. Networks can also be used to identify 'unknown unknowns'. For instance, network science can help identify where hidden nodes or connections are likely to be based on the functioning of the network. It can also be used to help predict the likely impact of removal of a specific node (e.g., by arresting a particular individual).

Professor Adam Joinson leads, and Brittany Davidson is funded by, the Understanding and Countering Online Behaviour CREST research programme at the University of Bath.

DOROTHY CARTER AND CYNTHIA MAUPIN

LEADERSHIP IS A SOCIAL NETWORK: IMPLICATIONS FOR SECURITY

It can take years to understand why and how certain individuals associated with terrorist organisations, such as Islamic State leader Abu Bakr al-Baghdadi (pictured), are able to successfully influence large swaths of people, and even longer to learn how to prevent them from doing so. Our research suggests that in order to understand leadership — both within terrorist organisations, as well as across the organisations striving to ensure the safety and security of our populations — we need to rethink traditional assumptions about leadership and view leadership through a social network lens.

What is leadership?

Traditionally, organisational researchers have sought to understand leadership by focusing on the traits or behaviours of individual 'leaders'. Leadership research has often progressed under the assumption that leaders possess some sort of formal authority over a set of subordinates, and that leaders and followers all share a single common group identity as in the case of the manager of a unit or the CEO of an organisation. Leaders in terrorist organisations often break traditional moulds with regard to scholarly views of leadership. Terrorist leaders derive much of their power by operating outside of normal societal constraints and hierarchies, and they often use informal means to influence others both within, as well as outside, of their immediate groups.

Certainly, terrorist systems rarely conform to traditional models of organisations developed for the industrial revolution era. However, even in 'traditional' organisations, such as the military, governments and corporations, leadership does not always fit neatly into formal organisational hierarchy charts. People often influence one another informally, and these informal influence processes are not always exerted in support of organisational goals.

Our work, along with other leadership scholars, strives to better understand leadership in complex organisational systems by recasting leadership as an emergent social relationship that arises as at least one person attempts to influence another and at least one other person grants the influence attempt. The participants in leadership relationships may or may not occupy formal positions of authority and/or share a common group membership. Clearly, in large and complex social systems, numerous people will participate in leader-follower processes in relation to one another, simultaneously, or over time. Thus, leadership relationships form a complex web or '***leadership network***' that emerges and evolves in response to changing situations.

Implications for security professionals

The view of leadership as a network yields at least three important implications for security professionals. First, when considering how leadership shapes the success or failure of any operation, it is necessary to go beyond the impact of any individual leader to consider the impact of the network of leader-follower influence relationships. Research suggests there are certain leadership network patterns that are more or less beneficial for collective outcomes, over and above the effects of any individual leader. For example, evidence shows that within small teams, a 'shared' pattern of leadership, where many members contribute to the leadership of the team, can have positive effects on team performance. Thus, targeting a single leader, or a few leaders, in a terrorist cell may not sufficiently alter the direction of the collective.

Second, in order to predict how and why influence will come about, we need to move beyond thinking only about the characteristics of potential leaders, such as their personality traits and experience. Like other types of social networks, leadership networks come about not only due to attributes of individual leaders, but also due to characteristics of both followers and of the social contexts they operate within, including group norms and the patterns of other networked social connections (e.g., advice, friendship, communication). Predictions regarding who will lead and who will follow, could be significantly enhanced by considering these multilevel drivers of leadership networks.

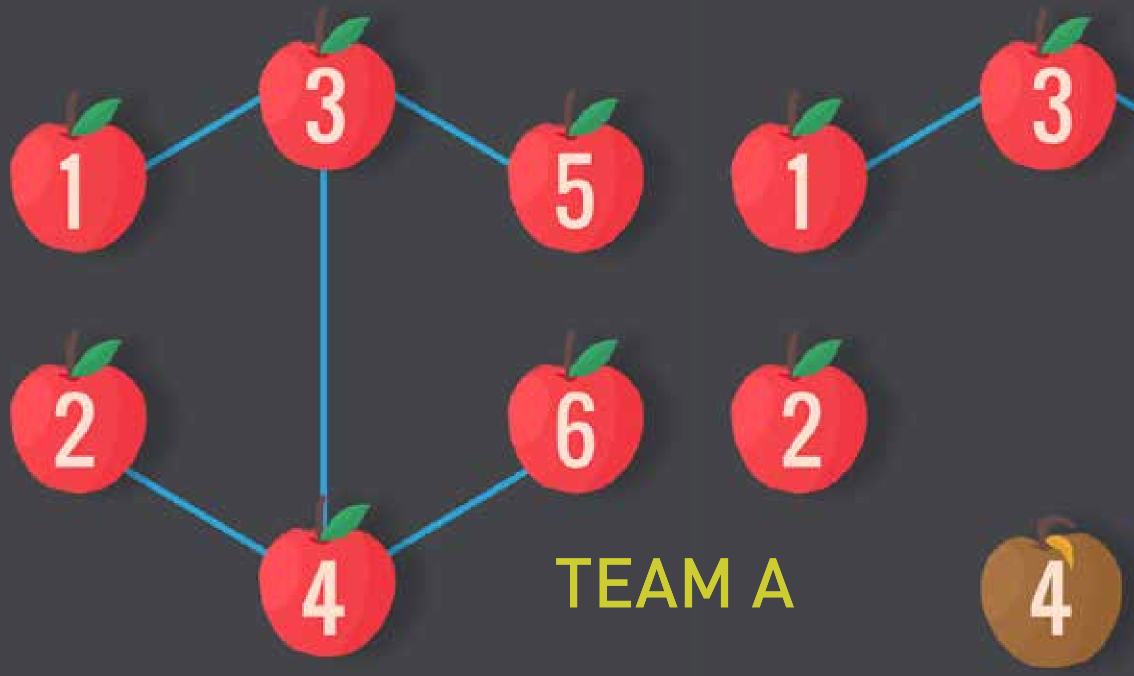
Finally, in order to remain adaptive and competitive in this challenging era for national security, we may need to re-think how we develop leadership within the organisations that ensure the safety and security of our populations. Our research surveying over 200 leadership development practitioners suggests that networks might be incorporated into leadership development in at least three ways. First, based on research linking certain central positions in other social networks with leadership influence, formal leaders should be trained to understand and leverage their own social networks to enhance their influence. Second, it is important to train individuals to understand the social and leadership relationships of others—both within as well as external to their own groups. By better understanding why, how, and among whom influence is likely to arise, formal leaders will be better able to leverage, and potentially alter, others' networks to enhance security. Third, given the link between leadership network patterns and collective success, leadership development might take seriously the challenge of creating entire systems of effective patterns of informal leadership connections. There is potential for leadership systems to be enhanced through organisational structures and work practices that foster social connectivity, as well as through team-training strategies targeting the leadership and teamwork skills of entire teams, or systems of teams.

Dr Dorothy Carter is an Assistant Professor of Industrial-Organisational Psychology and the Director of the Leadership, Innovation, Networks, and Collaboration Laboratory (LINC) at the University of Georgia.

Cynthia Maupin, M.S. is a Ph.D. student in Industrial-Organisational Psychology at the University of Georgia.

JEROEN DE JONG

USING NETWORKS TO PREDICT THE IMPACT OF ‘BAD APPLES’ ON TEAM PERFORMANCE



In the past few decades, organisations have increasingly relied on teams to structure their work. The main reason for increased reliance on teams is a large body of evidence that working together can deliver better outcomes compared to those of individual members; including more creative solutions, more innovative ideas, and more efficient task execution.

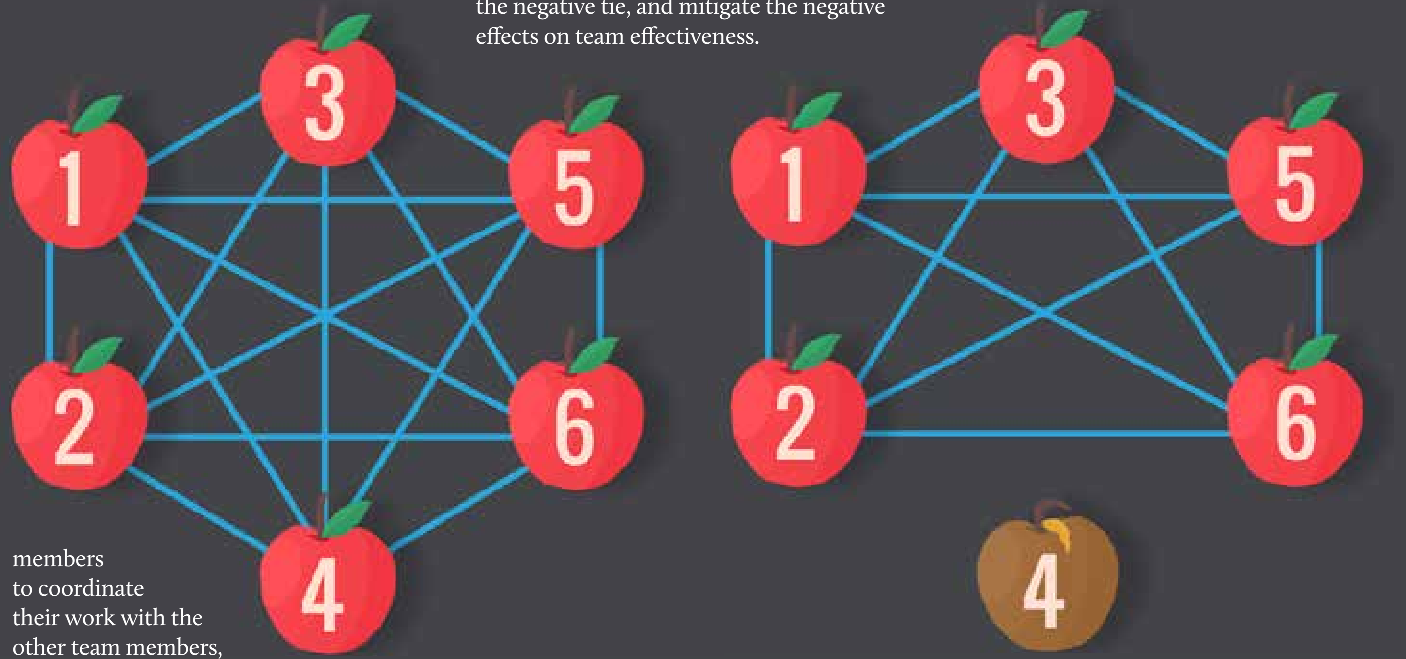
The main characteristics of teams are that they consist of two or more members who have goals, have a certain level of interdependence to reach that goal, and that there is a degree of social interaction required to reach their common goal. It is therefore critical to understand how team members coordinate, communicate, and share knowledge to reach their goalx.

To gain an in-depth understanding of these team processes, researchers often study the social network of the team.

A social network within a team is a set of team members that are connected by a set of relationships or ties. By asking each individual team member about the relationship they have with all other individual members of their team, researchers can get an insight into the structure of ties within the team.

These ties can be dichotomous (for example if the tie between two team members is present or not) and valued (for example, frequency of communication between team members), creating a network of ties between team members that characterise not only what kind of relationship two team members have, but also what kind of network the team has as a whole.

For example, Team A has one or two central members (member 3 and 4) who have ties to all other members, but these other members are not interconnected. Team B, on the other hand, has a social network characterised by frequent communication between all members of the team. Research has consistently shown that teams with more ‘dense’ social networks (in this case, Team B), that is, those with a high level of interconnectedness between members, are more effective compared to teams with lower density. A high level of interconnectedness between members allows for better task coordination, knowledge sharing, and responsiveness to external events. Because team members are interconnected, Team B can quickly communicate about their task and possible actions required to cope with unexpected events. Members 1, 2, 5, and 6 of Team A have to go through the two central team members to coordinate their work with the other team members, which is much less efficient.



Moreover, knowledge and influence are highly centralised in Team A, as the two central members can control what and when they communicate to their fellow team members.

Social networks can also be characterised by the type of tie between team members. For example, one member can be considered a source of advice for another member (advice tie), as a source of support (friendship tie), or as a tie that thwarts task behaviours among team members (negative tie). Again, research shows that teams with dense advice and friendship networks are more effective, as in these teams advice and support are available to all members, creating a cohesive and safe environment to express ideas and concerns. In contrast, teams with negative ties are less effective compared to teams without negative ties. When two team members dislike each other and engage in counterproductive work behaviour towards each other (e.g., they withhold information or even sabotage the work of the other team member) this disrupts the flow of communication and knowledge within the team. Moreover, the negative attitude of the negative tie can spill over to the rest of the team, decreasing cohesion and safety in the team. Research suggests, however, that strong ties between the other team members can help to bypass the negative tie, and mitigate the negative effects on team effectiveness.

Mapping the social network structure of the team can provide valuable information about team processes and effectiveness. Teams with dense social networks are able to coordinate the work and share knowledge effectively but are also able to cope with possible negative relationships in the team. Therefore, stimulating communication among all team members and allowing advice and friendship networks to develop are key conditions for effective teamwork, and even allow teams to work around the negative impact of a ‘bad apple’.

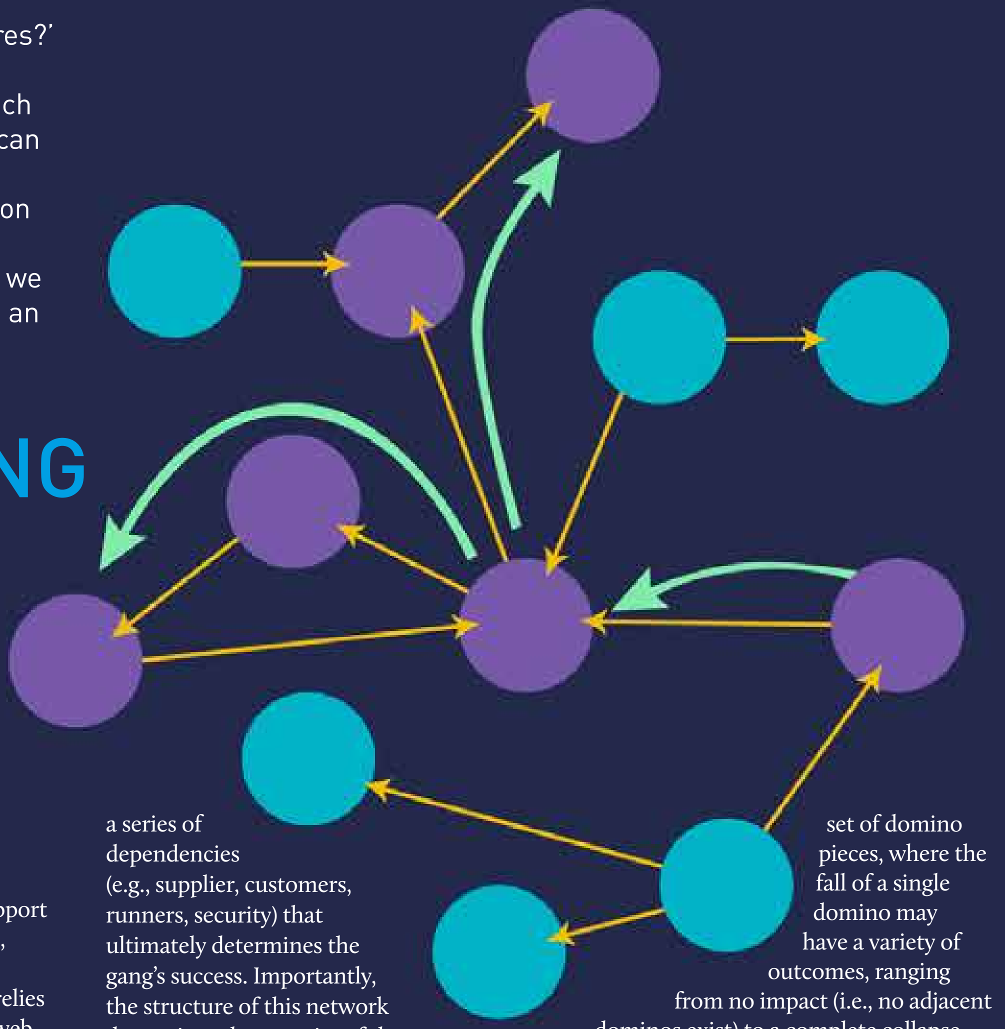
Dr Jeroen de Jong
Open University of the Netherlands

CHRISTOS ELLINAS

PREDICTING AND PREPARING FOR THE FAILURE OF COMPLEX SYSTEMS

Can Kim Kardashian's photo break the Internet? 'Who cares?' you may ask. Yet underlying this naïve question lies a much deeper and pervasive one – can a co-ordinated event single-handedly disrupt the operation of a complex system? And, importantly for security, can we predict and prepare for such an event happening?

CASCADING PROCESS



Systemic failures

The functioning of modern society largely depends on its capacity to support the global exchange of people, goods, money and information. Similarly, organisational performance heavily relies on our ability to manage a complex web of interdependencies as they evolve throughout time, whether they correspond to material flows (e.g., supply chains), activities (e.g., projects) or interactions (e.g., teams).

It's possible to understand the various interdependencies in a system in the form of a network, where nodes and links correspond to components and their respective interdependencies. So, in the case of a drug dealing gang, the group have a series of dependencies (e.g., supplier, customers, runners, security) that ultimately determines the gang's success. Importantly, the structure of this network determines the capacity of the system to sustain large-scale, systemic failures such as the loss of a key supplier or arrest of a leading member.

The dynamics that drive these systemic failures are generally attributed to two basic mechanisms.

The first mechanism corresponds to a cascading process, where a single node fails and has the capacity to affect subsequent nodes. In search of an analogy, consider a set of domino pieces, where the fall of a single domino may have a variety of outcomes, ranging from no impact (i.e., no adjacent dominos exist) to a complete collapse (i.e., first domino in a sequence). Examples of systemic failures that reside on this mechanism include: a single task failing, ultimately affecting the performance of an entire project, or a single contaminant eventually compromising the entire supply chain. In a security context, it is akin to the discovery of one member of a cell leading to the entire group being compromised as each person leads to another.

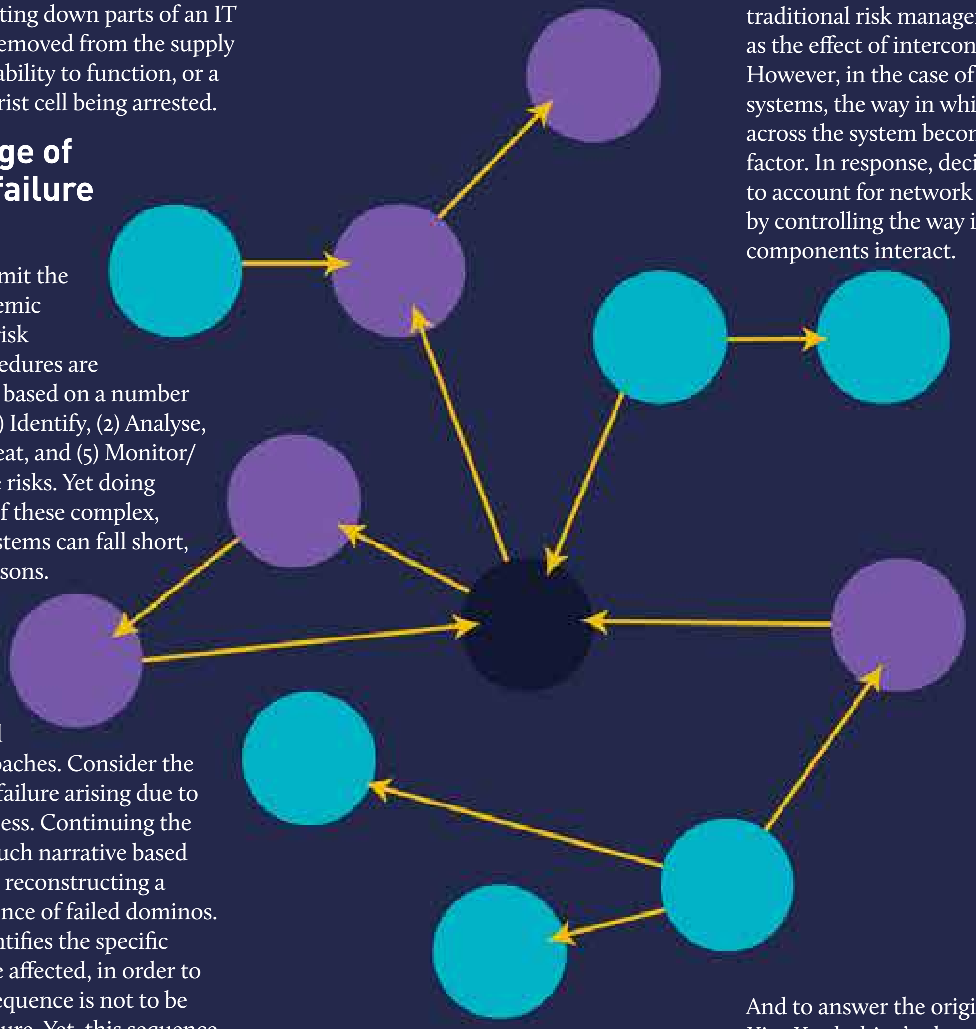
The second mechanism corresponds to the removal of individual nodes in an iterative manner. For example, consider a network where a node is selected and 'removed'. As a result, all links attached to this node are also removed, creating a 'structural hole' in the network. Repeating this process in a strategic manner can cause additional nodes to disconnect, ultimately bringing the entire system to its knees. Failures driven by this mechanism include: hackers targeting and shutting down parts of an IT system, a factory removed from the supply chain due to its inability to function, or a member of a terrorist cell being arrested.

The challenge of preventing failure spreading

In an attempt to limit the emergence of systemic 'domino' failures, risk management procedures are typically enforced, based on a number of general steps: (1) Identify, (2) Analyse, (3) Evaluate, (4) Treat, and (5) Monitor/Review all possible risks. Yet doing so in the context of these complex, interconnected systems can fall short, for at least two reasons.

First, identifying the cause of these systemic failures typically relies on narrative-based contingency approaches. Consider the case of a systemic failure arising due to the cascading process. Continuing the domino analogy, such narrative based measures focus on reconstructing a materialised sequence of failed dominos. By doing so, it identifies the specific dominos that were affected, in order to ensure the same sequence is not to be repeated in the future. Yet, this sequence is merely one manifestation out of all possible combinations allowed by the network, some of which are potentially more harmful. Hence, the risk of observing a large collapse of dominos has not been reduced, only the risk of encountering the same (or a closely resembling) one.

Second, evaluating the impact of a given risk can be exceedingly challenging. Systemic failures do not necessarily arise from large exogenous events nor require a set of extraordinary conditions. Rather, minor disturbances are sufficient in triggering both small, local and large, systemic failures. This is particularly important as the occurrence of a single node failing (or being removed) is a more probable failure scenario compared to other exotic ones.



NODE REMOVAL

Rethinking risk management

Network Science is helping us understand the limits of traditional risk management, along with paving new ways to account for its limitations. For example, in the case of densely-connected systems, we now know that the susceptibility to systemic failures is controlled by the stability of its individual components. In this case, traditional risk management can suffice, as the effect of interconnectivity is limited. However, in the case of sparsely-connected systems, the way in which links are spread across the system becomes a detrimental factor. In response, decision makers need to account for network effects by controlling the way in which components interact.

And to answer the original question, Kim Kardashian's photo release diverted roughly 1 percent of all internet traffic into the host webpage. Increased bandwidth requests cascaded throughout the server network, eventually slowing down the entire Internet. So in short, the answer is yes. A photo can really break the Internet.

Christos Ellinas
University of Bristol

THILO GROSS

THINGS THAT SPREAD: EPIDEMICS ON NETWORKS

Over the past decade epidemic processes on networks have become a hot topic in physics and mathematics. Researchers have gained surprising insights into biological epidemics and also a diversity of related phenomena, ranging from the spread of radical opinions to cascading failures in power grids. In an ever more connected society these insights are starting to make an impact.

One of the fundamental insights from physics is that very different systems sometimes follow the same mathematical equations. This is also true for simple epidemic models, which are studied increasingly because of their relevance for biological epidemics but also because they shed light on a wide range of other phenomena where 'things spread': computer viruses, forest fires, invasive species, and even to some extent corruption and criminal behaviour.

Avenues of transmission

To persist and propagate, epidemics need avenues of transmission. The more of these avenues that exist the higher the chance an epidemic will emerge, the quicker it will spread, and the bigger it will become. For instance, when humans first started to build cities they were afflicted by numerous outbreaks of previously unknown diseases that took advantage of the denser human proximity, and hence avenues for transmission, that city life afforded.

Superspreaders

Although the number of contacts through which a disease can be transmitted is the single most important determinant for outbreaks, the distribution of these contacts in the population takes a close second place. In many relevant networks, such as social contact networks and sexual contact networks, some individuals have very large number of contacts. These 'hub' individuals are for instance bus drivers, who, in a normal working day, have interactions with hundreds of different passengers. These high number of contacts with hubs come to bite us twice: Hubs are proportionally more likely to contract an epidemic disease, and once infected they are more likely to spread it. Due to this quadratic effect hub individuals become so-called superspreaders of epidemics.

Attacking networks

From the perspective of flu, washing your hands is an attack that removes links across which it can spread and getting vaccinated is an attack that removes a network node. The maths of stopping epidemics is thus the same that we use when we want to attack (or protect) other networks. The natural target for vaccination 'attacks' on a network are the superspreaders. At least in some models vaccinating the top 1% most-connected individuals has a greater impact on the disease than vaccinating the bottom 90%. This insight can be readily transferred to other applications, such as cyber security. In a company, the employees that regularly send out large number of mails and documents to multiple recipients are potential superspreaders of certain worms and viruses. So, it is sensible to ensure that these employees particularly have received training that enables them to recognise these threats.

Fighting fire with fire

In the networks that are relevant to biological epidemics we do not know with certainty who potential superspreaders are. Privacy concerns and the scale of the required effort prevent us from creating detailed maps of contact networks. However, if an epidemic can find highly connected individuals by spreading over the links, so can vaccination campaigns.

One suggestion is to have a campaign where recipients of a vaccination can nominate friends to be offered a free vaccination. In this way the vaccination campaign itself starts to behave like an epidemic, and thus preferentially affects the network hubs. While similar ideas are now regularly used in viral marketing, their application to epidemics comes with a big caveat: Such campaigns will only work for diseases where the contact network relevant for disease transmissions is closely aligned with the contact network for vaccinations. Our bus driver from the previous example is a likely hub in the epidemic network, but not necessarily in the nomination network.

The future

In the future the size and density of the human population will likely continue to increase, also the rise in long distance travel will continue leading to ever more tightly knit global contact networks across which epidemics can spread. Aggravating this situation is the misuse of antibiotics which has eroded our main line of defence against epidemics. Finally, history has shown that new epidemics often emerge in response to environmental changes that bring us into contact with new pathogens. In the face of increasing connectivity and accelerating environmental change the emergence of new major epidemics in the near future is foreseeable.

While the battle against future epidemics will mainly be fought by biologists rather than mathematicians, research in networks can help us to predict outbreaks better and may increase the efficiency of vaccination campaigns, saving money and lives. At present, the biggest unknowns in this field concerns human behaviour.

What is the structure of human social networks, how do they form and change in time, and how do they respond to major events such as epidemics? Present and future progress on this question will improve our abilities to combat epidemics, and also aid us in many other security-relevant contexts.

Dr Thilo Gross, Faculty of Engineering, Department of Engineering Mathematics, University of Bristol

MIA BLOOM

ISLAMIC STATE MESSAGING ON TELEGRAM

A persistent feature of terrorism is communicating a message. Whether broadcast in ancient times by word of mouth – the Assassins perpetrated attacks on feast days to maximise publicity – or televised – Palestinian militants' chose the 1972 Olympics to maximise news coverage – attempts to amplify terrorist messaging are commonplace.

With the popularity of the Internet, and since then, social media, terrorist groups embraced a virtual world and, for many, the online space became their default platform for activities from recruitment, to strategic communications, to raising funds.

Sunni extremist groups such as al-Qaeda (AQ) and the Islamic State group (IS) exploit online platforms to broadcast their messages and disseminate propaganda. Jihadi supporters have constructed an interconnected 'imagined community' fostering identity, group cohesion, engagement, while simultaneously encouraging attacks using a variety of digital platforms. IS propagandists and sympathisers were early adopters of Twitter and Facebook in the construction of their 'virtual caliphate'. Investigations into terror plots in Russia have demonstrated that Telegram is playing a crucial role in such activity; in contrast to it being a platform for merely spreading propaganda, the platform is increasingly recognised as a source for recruitment and coordination of terrorist plots and attacks in Western Europe.

Telegram is an instant messaging service, providing optional end-to-end encrypted communications. It is free and open and has no limits on how much data individual users can download or share. Telegram was launched in 2013 by developers Nikolai and Pavel Durov, the founders of VK (ВКонтакте or VKontakte), Russia's largest online social network. In 2016 Telegram announced that it had more than 100,000,000 monthly active users, and as a result Telegram is delivering 15 billion messages daily.

As social media policing became more aggressive in the past two years, Telegram has largely replaced IS's online presence on open platforms like Facebook and Twitter. Several thousand channels and groups ensure that IS branded content, videos, manuals, speeches and writings, are disseminated without interruption. Without research into the dark web, IS social media can appear to be degraded or in decline when, upon closer inspection of their materials in Arabic, their media operations and strategies have simply evolved. IS Telegram has constructed an online 'imagined community' allowing supporters to overcome problems of collective action in planning terrorist attacks.

In my research, I explore how the chat rooms and channels grow, how they advertise their content, recruit followers, and resurface after aggressive deletions by security and counter-terrorism personnel. In addition to examining the content and dissemination metrics, my research team observes and analyses the psychologically addictive qualities of the platform and the ways in which behavioural design is used to increase engagement and manipulate reward structures.

Previous studies have examined the effects of excessive social media usage on human behaviour, suggesting that there are addictive properties intentionally designed to maintain user attention and foster both psychological and emotional dependence on the virtual world. IS achieves this by limiting the time that new content, for example a video, is available on its channels. Users have to check the channel regularly to ensure they don't miss this content.

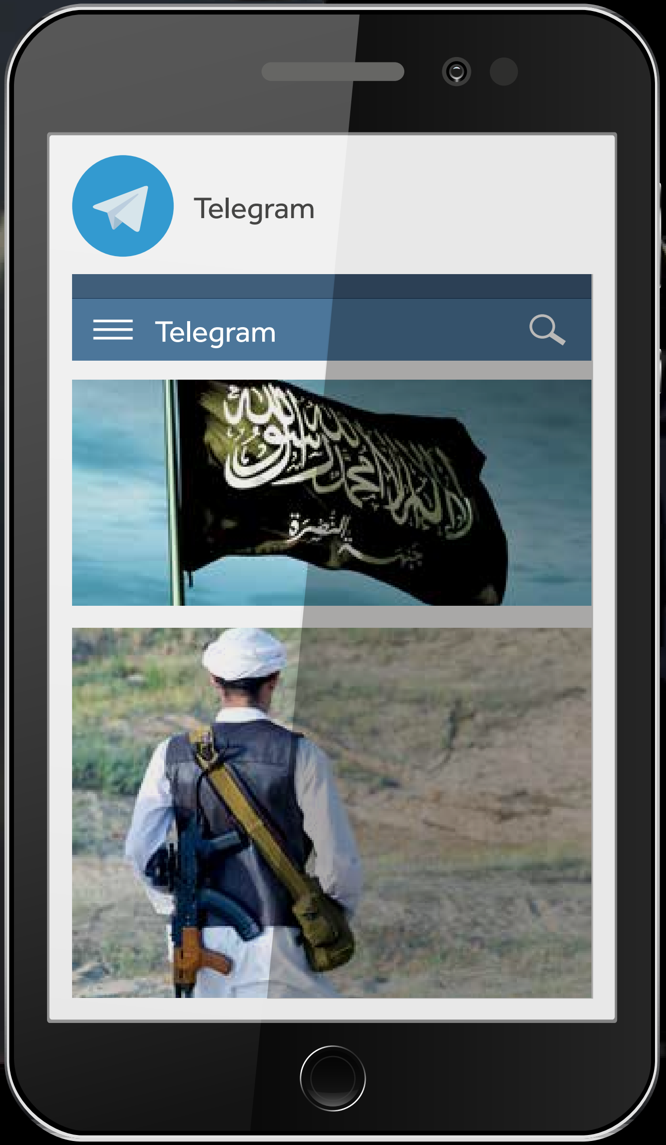
This design combines the fear of missing out (FOMO) with a 'variable interval schedule of reinforcement'. In practice, this means content reinforces the commitment of the end-user, is varied and is stimulating, abundant, constantly changing and allows only a limited time for response. These qualities are present in other compelling (and addictive) activities (e.g., slot machines, online gambling and mobile gaming). Such dynamics do not merely encourage behavioural commitment, but foster dependence and addiction.

Why is it important?

Telegram provides key insights into where IS will militarily expand next and allows us to observe and disaggregate the micro-trends that are occurring regionally and sub-nationally. For example, by monitoring the chatter on the channels (and the growth of channels posting) in Bahasa, you can track how the group appears to be expanding in the Philippines.

It is important to understand how terrorist groups use networks to disseminate and recruit new members, but also how best to disrupt and/or to predict changes in social media. Most of all, in order to counter terrorist propaganda, it is crucial to understand how that propaganda is created and disseminated, and in particular, to urgently understand what strategies IS is deploying to harness and sustain the continued engagement of their online users.

Dr Mia Bloom is Professor of Communication at Georgia State University. She is currently researching how Jihadi groups are using social media to build their "Virtual Caliphate" as part of the Minerva Research Initiative grant #N00014-16-1-3174. CREST has a guide to messaging applications, including Telegram, which you can download from www.crestresearch.ac.uk/resources



MARTIN EVERETT

COVERT NETWORKS

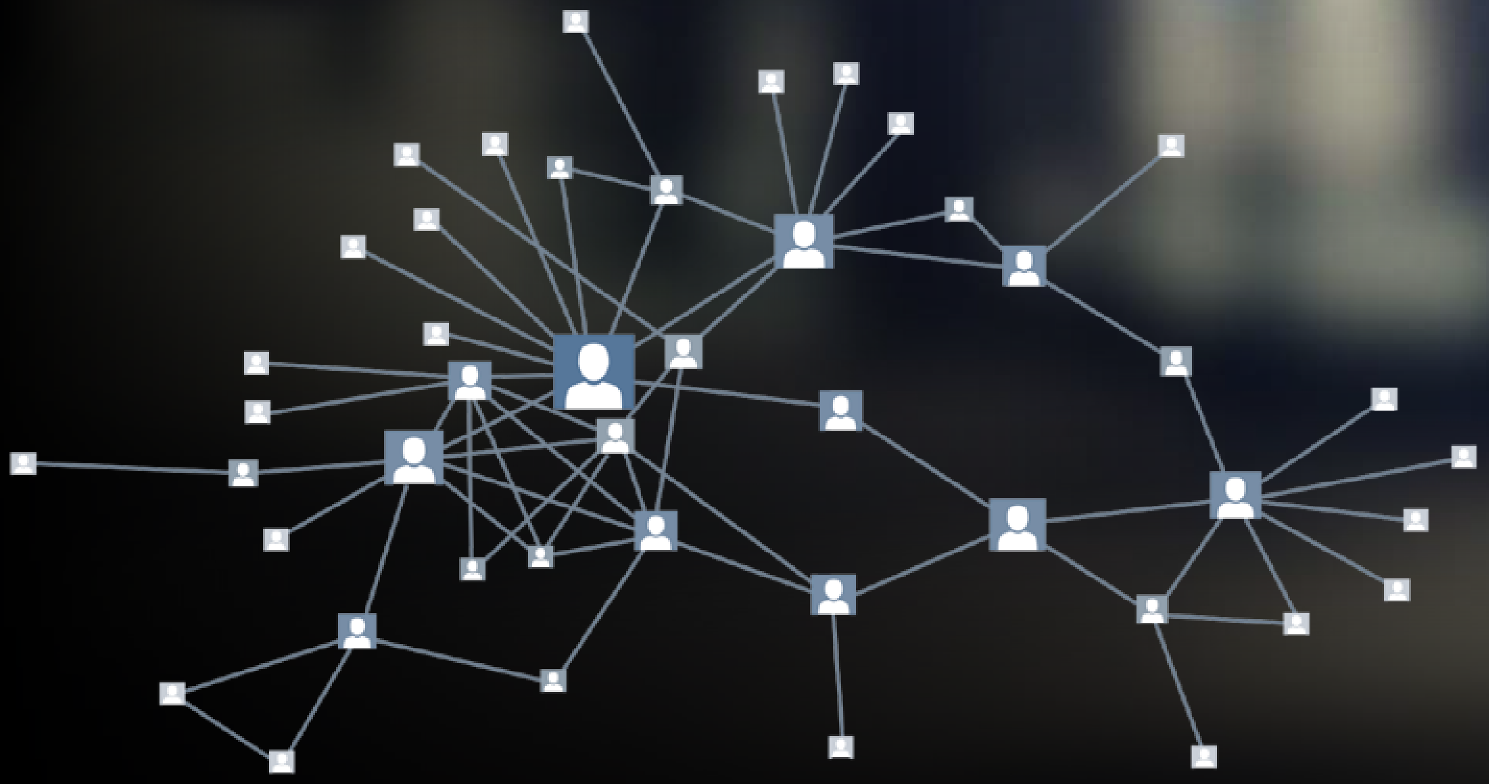
How can social network analysis help with the study of terrorist and criminal networks? Martin Everett researches covert, or dark, networks and presents an example based on the Provisional Irish Republican Army (PIRA).

Social networks are a way of thinking about social systems that focus on the relationships among the entities that make up the system, these entities can be people or collectives such as organisations, or families, and are referred to as actors or nodes. The nodes often have characteristics – typically called 'attributes' – and these can be categorical traits, such as having a conviction, or continuous attributes, such as being 52 years of age. The relationships connecting the nodes can be of many different types and each relation gives rise to a separate network. Examples of relationships are 'friendship', 'talks to', 'associates with', as well as secondary types of tie such as 'arrested with', 'attended the same church as', 'belonged to the same club as'.

As an example of a network, the diagram below is the main connected portion of part of the PIRA. The nodes are known PIRA members and the relations are one or more of the following: 'took part in an active mission', 'were friends before joining', 'are blood related directly' or 'are related by marriage'.

Data in this case was obtained from a variety of accounts and historical documents. In other examples data has been obtained from wire taps, via co-arrest and co-offending or from public sources. A collection of publically available networks that describes the data and how it was sourced is available at: *https://sites.google.com/site/ucinetsoftware/datasets/covert-networks*

Once the data is in network form an analyst has a number of tools that can be used to help uncover important features. A simple visualisation of the data is often helpful in identifying portions of the network of interest.



For example, nodes with a high number of connections could well indicate a level of activity consistent with a co-ordination or leadership role.

One consistent finding in social network research has been that people tend to associate with people like themselves. This includes criminal and terrorist actors, and so if we have a known criminal or terrorist in a network it would be worth looking closely at who they are connected to because those may be the most likely to be involved in similar offending. This approach has been successfully applied to fraud networks.

There are a number of techniques used by analysts to uncover important properties of the network. Two are particularly important. The first is to identify actors who occupy structurally important positions. As already discussed, looking for nodes with a large number of connections is one such example. A subtler example is to identify nodes who are well placed to capitalise on any information flowing through the network. This is called betweenness centrality and in our diagram I have sized the nodes proportionally to this measure. In real life applications, including this example, such nodes are often those in leadership positions and so network analysis can help determine on which actors to target resources.

A second useful technique is to identify portions of the network in which actors are more closely associated with each other than with other actors. Such portions are called cohesive subgroups or communities. This is important as offending tends to be organised in clusters, so identifying the clusters in the network again allows resources to be targeted.

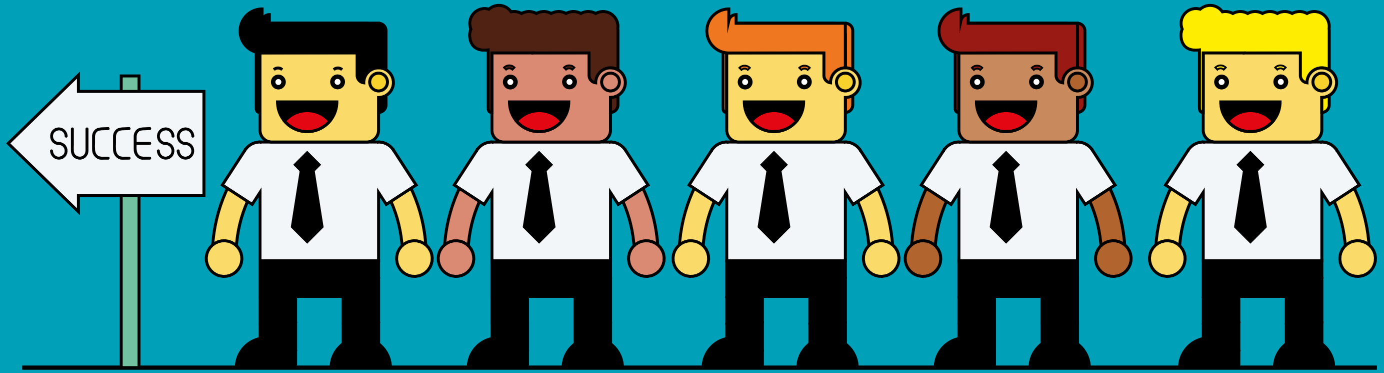
Professor Martin Everett
Mitchell Centre for Social Network Analysis, University of Manchester

ROSALIND SEARLE AND CHARIS RICE

TRUST AND INSIDER THREAT: ENSURING WE DON'T LOOK BACK, OR FORWARD, IN ANGER

How can networked trust in organisations, both between employees and processes be maintained, especially during times of great change?

Rosalind Searle and Charis Rice are leading a new project to find out...



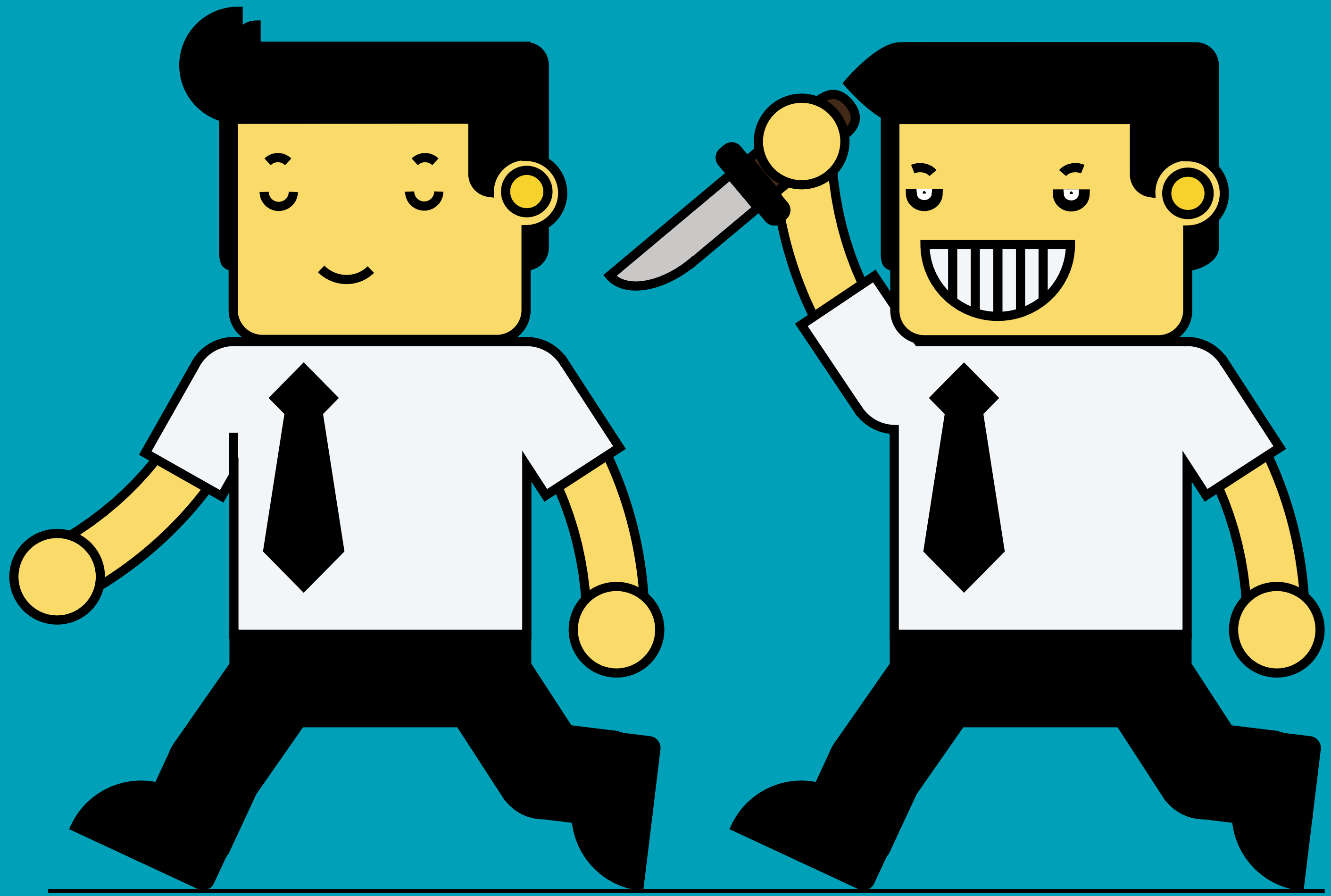
Trust is an important resource in managing our dependencies on others; it reduces our uncertainty, freeing up cognitive resources to allow more focus on the task in hand. Trust emphasises an individual's willingness to be vulnerable, based on positive expectations of the intentions or behaviour of another to act at best in our interest, or at worst benignly. Such confidence stems from two dimensions: first, a rational cognitive-based trust derived from the trusted party's past performance. It comprises insights into their skill and competence. It can extend to an organisational-level to include the systems and processes an organisation uses. The second dimension, affect-based trust, concerns the care, value and respect the other party shows us – a sense that they have our best interests at heart, so promoting greater levels of commitment.

In contrast, distrust involves pervasive negative expectations of the motives, intentions or actions of others. Trust, therefore, is to a large extent derived from the past, a bit like driving by looking in a rear view mirror, which is fine as long as the road remains the same. But what happens when an organisation faces things for the first time, such as having to make redundancies?

Periods of change can be important crucibles for trust and distrust. Change disconnects people from their previous employment roles. It alters their relationships with close colleagues through whom their organisational identity is nested. More insidiously, the way change is managed can expose inequalities and inconsistencies leaving those affected feeling less committed. Transformations can create the emergence of internal threats to organisations, as longstanding employees become disgruntled, angry and sufficiently disengaged to behave in counterproductive ways as a form of redress, or worse, revenge.

Suddenly model employees can become distrustful. These behaviours can be small scale such as time wasting, or more serious insider threat activities such as destroying systems or leaking confidential information; they must therefore be considered within a broader context of threat to wider publics and national security. So how can organisations stay secure during times of change? We propose, through understanding the elements which support trust development, maintenance and its repair to avoid the shift to distrust.

Recent studies have shown control systems complement trust. Input controls provide re-assurance determining who enters the organisation, while output control covers what is done. Process controls concern how things are done, allowing employees to better navigate their way and creating consistency across different components of large organisations.



Finally, sanctions and punishments show the seriousness directed at those who deviate. Transparent and fairly-used controls are enhancers of trust levels. Employees pick up clues and signals about organisations and their key agents during the course of their employment. While those at the top of the organisation are important, the line manager plays a critical role in such signalling.

Line managers who lack competence emerge as less of a liability for trust than those without integrity. Effective line managers are important in promoting positive work attitudes, enhancing job satisfaction, reducing decisions to quit, and increasing organisational citizenship and commitment. Even more security is gained through ensuring an employee feels trusted by their line manager. Co-workers also play an important role, they share insight and create a group level perspective on the local and wider organisation.

The implications for organisational managers is that, particularly during times of uncertainty or change, attention should be devoted to managing expectations through clear and ongoing communication. This includes, perhaps paradoxically, being transparent about when and why it might not be possible to be fully transparent. Leaders must pay as much attention to making organisational decisions in a fair manner, as to the outcome of the decision itself. As responsible members of organisations, we can all learn more about our colleagues and employees by being vigilant to individuals' emotions and the behaviours which may exhibit warning signs of threat. All of this can be done by enacting both cognitive and affective trust and by considering what signals we send employees both in times of stability and in change.

Professor Rosalind Searle and Dr Charis Rice are based at the Centre for Trust, Peace and Social Relations at Coventry University. This project is funded by the Centre for Research and Evidence on Security Threats, more information can be found here: www.crestresearch.ac.uk/projects/counterproductive-work-behaviour

STEPHANE BAELE, KATHARINE BOYD AND TRAVIS COAN

EXTREMIST PROSE AS NETWORKS

USING CO-OCCURRENCE NETWORKS TO MONITOR EXTREMIST COMMUNICATIONS

A well-developed body of research demonstrates that network analysis offers considerable insight by studying the links between political actors, groups, and entities. At the same time, there is also a growing body of work that focuses more specifically on extremist networks. While much of the published research on extremism centres on 'social networks'—i.e., networks of individuals—our research takes a different approach, focusing instead on the network of words and concepts embedded in extremist propaganda. The results suggest that viewing textual information through the lens of network analysis offers a powerful way to complement existing approaches to monitoring and analysing extremist communication.

There are a number of different ways to extract relational information from written communication, but the most common approach focuses on the concept of word (or phrase) 'co-occurrence'. This approach assumes that co-occurring words also tend to share a common meaning or represent a common theme. For instance, our research on Islamic State (IS) propaganda demonstrates the words 'American' and 'crusader' often co-occur, while also sharing a common reference to an important outgroup. Despite its simplicity, the idea of co-occurrence provides the foundation for many of the most commonly employed text mining algorithms.

Using the basic idea of word co-occurrence, it is relatively easy to develop a network-based approach to examining textual information. In a co-occurrence network, each of the words in a body of text represent the 'nodes' in the network, and any words that commonly appear close together represents an 'edge' connecting two nodes. The connections (or edges) in these networks can be 'undirected' (i.e., simple cooccurrence) or 'directed' (i.e., represent a dependency relationship between words – for instance 'effeminate scholars' in IS prose). Importantly for researchers and practitioners, text networks offer a flexible and relatively quick way to analyse large quantities of extremist propaganda by drawing on recent advances in the field of network science.

To gain a better sense of how this analysis works in practice, consider a co-occurrence network for the IS magazine, Dabiq (issues 1-15). A visual representation of the network is provided in Figure 1. Through our research, we observe five major 'communities' or themes: 'outgroup' (portrayals of the identity and evil actions of IS' perceived outgroups), 'jihad' (descriptions of IS' war against these enemies), 'Caliphate' (depictions on the perfect life and mores in the established Caliphate), 'legitimation' (discussions of the deeds and sayings of Muhammad and his companions in ways that legitimise the establishment and actions of IS), and 'sins' (debates on the major sins such as 'kufr' and 'shirk', associated with the 'corrupt' 'Western' and 'Christian' world). These themes are closely connected through important bridge words (e.g., 'hijrah' between 'outgroup' and 'Caliphate', 'Dabiq' between 'outgroup' and 'legitimation,' and so on) and thus create a coherent system of meaning.

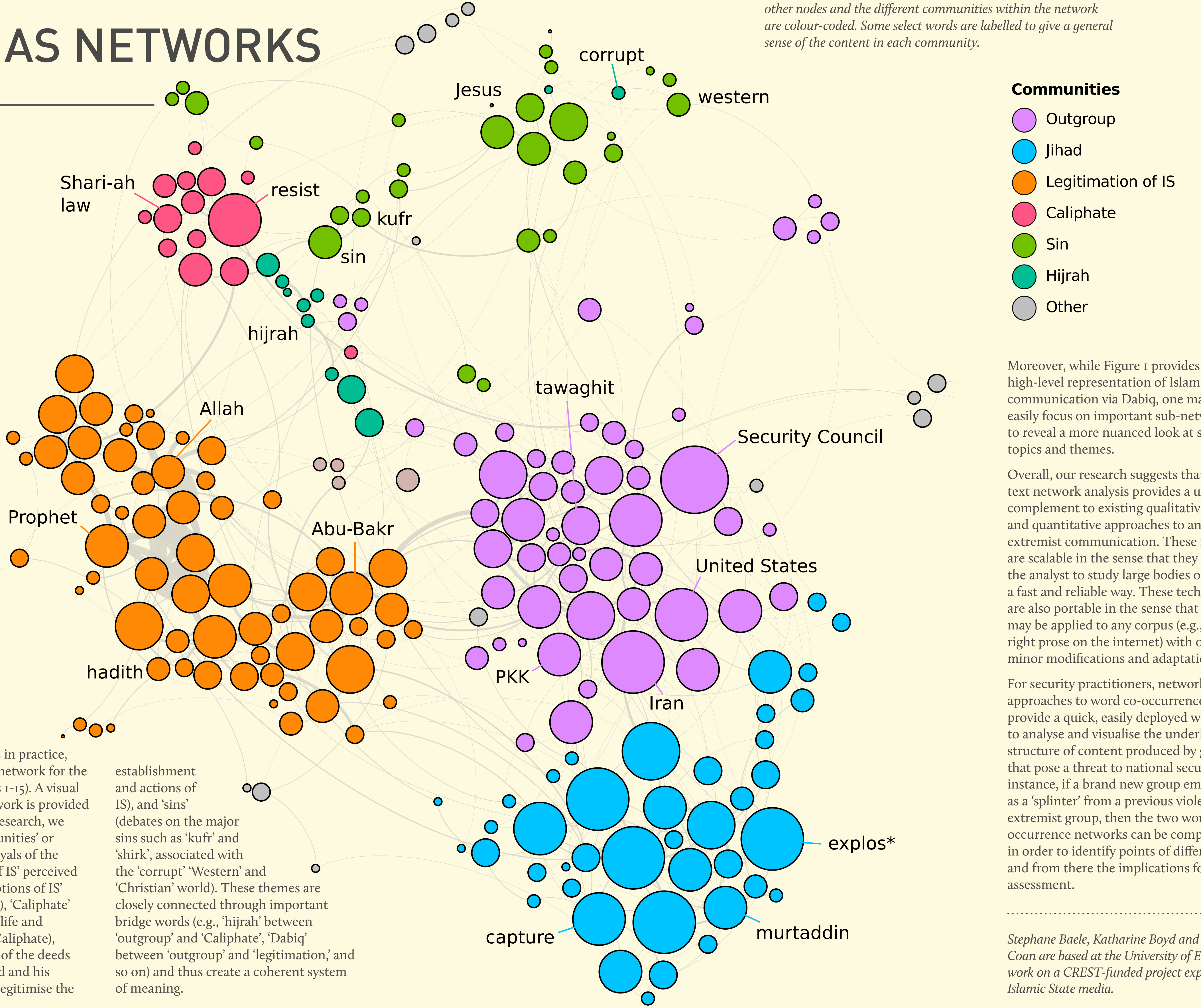


Figure 1: Co-occurrence network of Dabiq magazine, issues 1-15. Node size is determined by the number of connections it has with other nodes and the different communities within the network are colour-coded. Some select words are labelled to give a general sense of the content in each community.

Moreover, while Figure 1 provides a high-level representation of Islamic State communication via Dabiq, one may easily focus on important sub-networks to reveal a more nuanced look at salient topics and themes.

Overall, our research suggests that text network analysis provides a useful complement to existing qualitative and quantitative approaches to analyse extremist communication. These methods are scalable in the sense that they allow the analyst to study large bodies of text in a fast and reliable way. These techniques are also portable in the sense that they may be applied to any corpus (e.g., far-right prose on the internet) with only minor modifications and adaptations.

For security practitioners, network approaches to word co-occurrence provide a quick, easily deployed way to analyse and visualise the underlying structure of content produced by groups that pose a threat to national security. For instance, if a brand new group emerges as a 'splinter' from a previous violent extremist group, then the two word co-occurrence networks can be compared in order to identify points of difference, and from there the implications for threat assessment.

Stephane Baele, Katharine Boyd and Travis Coan are based at the University of Exeter and work on a CREST-funded project exploring Islamic State media.

KATE MUIR

WHAT IS RAPPORT, AND HOW CAN YOU INCREASE IT?

Have you ever met someone and just immediately 'clicked' with them? You felt at ease, the conversation flowed, and you felt happy and comfortable in their company. If so, you have experienced that elusive and yet vital component of a good relationship: rapport. Rapport has been defined as perceived closeness, harmony and trust, built through verbal communications and self-disclosure.

Rapport has also been described as consisting of mutual attention (the degree of involvement between conversationalists), positivity (the emotional tone of the conversation) and coordination (reciprocity in responses, synchrony or accommodation). The components of rapport are created via non-verbal and verbal behaviours expressed by the individuals in the conversation.

Why should we care about rapport?

Perhaps unsurprisingly, rapport is positively related to the quality of relationships, and other outcomes, in a variety of settings. For instance, in the workplace, organisational success and job satisfaction is reliant on perceived feelings of closeness felt between supervisors and subordinates. Crucially, rapport is considered important to investigative interviewing for law enforcement and intelligence gathering purposes, as rapport between the interviewer and interviewee can increase the amount of information provided and engender greater cooperation. However, intelligence and law enforcement interviewers do not always succeed in maintaining adequate levels of rapport. So, by determining how people achieve rapport in conversations, we may be able to infer the means to strategically increase feelings of rapport.

Measuring rapport

The first step towards strategically enhancing rapport is to figure out how to measure it. This is a tricky question, as attributes such as affinity or harmony between individuals are not easily measured or quantified. Nonetheless, research suggests that various cues exhibited by conversationalists can indicate the presence of rapport. Behavioural cues such as gesturing, backchanneling, direct eye contact, and postural mirroring are good predictors of rapport. However, behavioural cues to rapport can be sensitive to the social context. For instance, these cues were good predictors of rapport between dyads who were debating (a competitive conversation) but not when dyads were planning a trip (a cooperative conversation).

Subjective cues, on the other hand, are those which are not perceived directly but which are inferred; such cues include psychological states (e.g., enjoyment, involvement, or nervousness) or latent psychological traits (e.g., agreeableness, dominance, or expressivity) which can be inferred from behaviours, facial expressions, and movements. Subjective cues can help outside observers form more accurate judgements of the rapport felt between conversationalists, suggesting subjective cues may actually be more useful in measuring rapport.

How to enhance rapport

Practically speaking, there are several ways to strategically create or enhance rapport. Agreeing with your partner and providing positive reinforcement have been associated with feelings of rapport and affiliation. Personal disclosure (providing personal information) in conversations has also been linked to rapport, and is thought to work by enhancing positivity in the conversation. Other research indicates that synchronising verbal and non-verbal behaviours via strategic mimicry acts to increase rapport.

Although 'synchrony' often refers to wider level coordination (in terms of turn-taking, and reciprocity in responses), synchrony at the word level has also been associated with increased rapport. Where conversationalists change their use of a particular class of words (function words such as 'the', 'and', 'in', 'she', 'have') to be similar to one another, this has been associated with increased perceptions of rapport. Further, these beneficial effects of word synchrony upon rapport are apparent where non-verbal signals are greatly reduced, such as in computer-mediated communication. One proposal for the mechanisms underlying the effects of word level synchrony is that it helps to establish two of the components of rapport, coordination and positivity.

There is still a lot of work to be done in defining and measuring rapport. Much rapport research has focused on non-verbal behaviours expressed in face-to-face conversations. However, given the increasing prevalence and importance of relationships formed and maintained online, it is just as important to study the verbal behaviours and responses that constitute rapport. Measuring and strategically increasing synchrony and coordination in word use has promise in this area, but does not always influence reported rapport. Some researchers suggest that synchrony in word use represents engagement in the conversation, rather than the formation of rapport.

In addition, most rapport research uses strangers as participants, but the behaviours that create or express rapport are suggested to change along the timeline of a relationship. Clearly, further research into the nature of rapport, its behaviours and how to assess if rapport has been formed or not is necessary if we are to successfully harness rapport as a strategic tool.

Kate Muir
University of Bath

MICHELE GROSSMAN AND PAUL THOMAS

COMMUNITY REPORTING – THE KEY TO DEFEATING TERRORISM?

The recent spate of terrorist attacks in the UK and elsewhere highlights more than ever what many police, researchers and policy makers have been saying for some time: Early intelligence from communities, especially those 'intimates' close to people who may be radicalising to violence, is crucial for the early disruption of terrorist plots.

A good number of terrorist actions in many countries have been prevented because family or friends have come forward to authorities with information that has prevented attacks from occurring.

However, until recently virtually no public research had been conducted that helped us understand what the experience of sharing information with authorities was like for family members and close friends. Agencies and policy makers had little insight or evidence for what helped facilitate early reporting; what the thought processes and dilemmas for reporters are; what barriers to reporting might exist, and how to overcome them; and, critically, whether existing systems for receiving, triaging and acting on information from families, close friends and communities might be helping or impeding the flow of essential information to the right places at the right time.

A 2015 government-funded academic study in Australia was the first to ask these questions directly and to develop an evidence base from which to consider whether current approaches and expectations around what the researchers called 'intimates' reporting were working, and if not, what needed to change. This pilot study interviewed 33 Australian community members and government stakeholders with a high level of knowledge and contact around community reporting experiences.

For individuals, the findings confirmed that people largely report on those close to them out of care and concern for the person radicalising to violence, as well as fear of the damage or harm they may cause to others. Worries about targeting, stigma and disproportionate responses by police if their fears are unfounded can inhibit reporting. And, significantly, they have an overwhelming preference for face to face reporting, rather than by telephone hotline or online web-based channels. Trust and transparency were the key ingredients people wanted to see as reassurance during the process, and for this reason there was a strong preference for reporting to community-based intermediaries rather than directly to authorities. The study results also highlighted the significant isolation and conflict many felt when considering the personal impacts of sharing what they knew, or suspected, with authorities. These included feelings of guilt, shame, loss of social belonging and betrayal: in other words, 'knowing' they were doing the right thing but nevertheless 'feeling' it was wrong.

However, beyond individual experiences, the Australian study also revealed key issues at the level of current systems and structures around reporting interfaces with authorities. The most important of these were indications that people were confused or unsure of how to report, when and to whom.

The second key issue was what the study called 'the leaky pipeline', in which initial or tentative efforts to share information, say with local police, saw those reporting bounced around from one agency or telephone service to another. The leakier the pipeline, the easier it is for people to lose heart, second-guess their decision to report and drop out of the process.

In the UK, a current study is now underway, funded by CREST – the Centre for Research and Evidence on Security Threats. It expands and develops the approach of the Australian study through a sample of 75 community members and professional practitioners, with a particular focus on young adults, matching the demographic profile of many plotters and those who travelled to Syria.

The UK study's preliminary findings suggest we need to re-examine policy and practice approaches around two key issues. First, sharing concerns with authorities about an 'intimate' is likely to be the last resort, with respondents much more likely to seek help from figures of authority within communities first.

This suggests that policy needs to acknowledge this reality and work in partnership with community organisations – the State needs to show more trust in community organisations as partners in terrorism prevention in the same ways it has done around hate crime reporting. This obviously raises issues around the current image and public understanding of the UK's Prevent strategy. Respondents would also consider sharing concerns with trusted professionals, such as university lecturers and doctors.

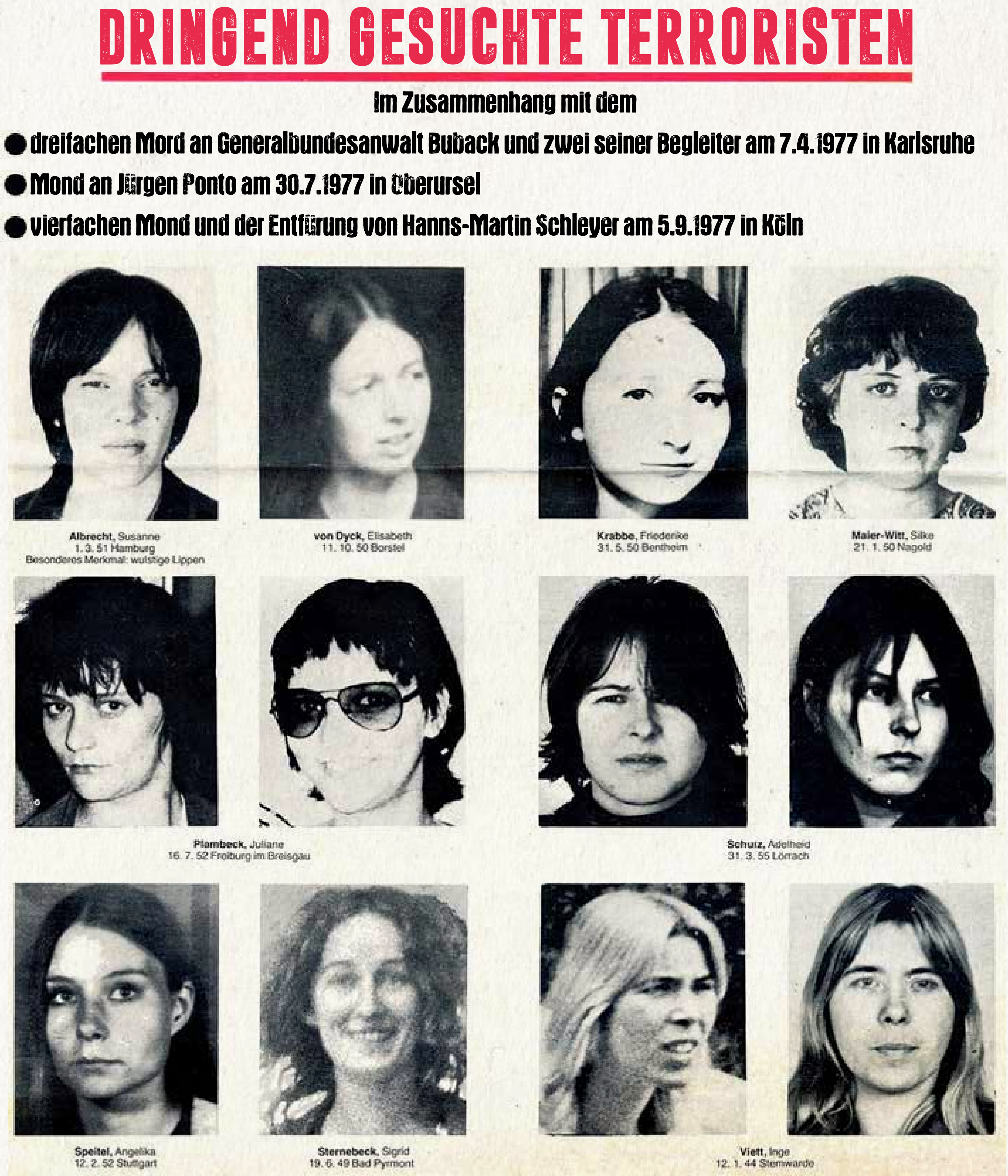
Second, reporting processes around terrorism are not clearly understood by community members or professional practitioners and need to be both strengthened and clarified. As in Australia, respondents in our current study express a strong preference for face to face reporting – they largely do not trust on-line or telephone based methods. This clearly raises issues about the local availability of policing services and of the training and preparedness of front-line policing personnel to receive and respond appropriately to reports of concern. It is in all our interests that this sort of research evidence can help strengthen approaches that enable community sharing of concerns about potential or existing terrorist activities and threats, to support early intervention.

Professors Michele Grossman (Deakin University, Australia) and Paul Thomas (University of Huddersfield, UK) are funded by the Centre for Research and Evidence on Security Threats. You can read more about their research at www.crestresearch.ac.uk.

KATHARINA KARCHER

CAN FEMALE PARTICIPATION IN POLITICAL VIOLENCE LEAD TO SOCIAL PROGRESS?

What role can women play in terrorist groups, how might that be reported and can it help pave the way for women in other spheres of society? Dr Katharina Karcher, from the University of Cambridge, addresses these questions based on her research on the Red Army Faction.



DRINGEND GESUCHTE TERRORISTEN

Im Zusammenhang mit dem

- dreifachen Mord an Generalbundesanwalt Buback und zwei seiner Begleiter am 7.4.1977 in Karlsruhe
- Mond an Jürgen Ponto am 30.7.1977 in Oberursel
- vierfachen Mond und der Entführung von Hanns-Martin Schleyer am 5.9.1977 in Köln

Albrecht, Susanne
1. 3. 51 Hamburg
Besonderes Merkmal: wulstige Lippen

von Dyck, Elisabeth
11. 10. 50 Borstel

Krabbe, Friederike
31. 5. 50 Bentheim

Maier-Witt, Silke
21. 1. 50 Nagold

Plambeck, Juliane
16. 7. 52 Freiburg im Breisgau

Schulz, Adelheid
31. 3. 55 Lörrach

Speitel, Angelika
12. 2. 52 Stuttgart

Sternebeck, Sigrid
19. 6. 49 Bad Pyrmont

Viett, Inge
12. 1. 44 Sternwarde

On 30 July 1977, Susanne Albrecht paid a visit to the villa of the German banker Jürgen Ponto, a good friend of her father's. According to witnesses, the young woman, accompanied by a 'decently dressed' couple, brought Ponto a bunch of wild roses. When he opened the door to welcome the visitors, they threatened him with guns and tried to abduct him. Ponto resisted, and was shot by the intruders. Two weeks after the attack, the left-wing terrorist group Red Army Faction (RAF), also known as the Baader-Meinhof gang, claimed responsibility for the killing.

The violent conflict between the RAF and the West German State, which had started with an armed raid in 1970, reached a dramatic peak in 1977. Jürgen Ponto was the fourth of ten RAF victims that year, and newspaper and other public responses to the Ponto murder show that it was not the brutality of this and other attacks alone that made the RAF Germany's most notorious terrorist group. In 1977, women clearly outnumbered men on the RAF wanted posters (see image), and their active participation in attacks was perceived as a violent transgression of and threat to the prevailing gender norms. An article published shortly after the Ponto killing illustrates this point. Here, the (male) author asked polemically: 'must every citizen worry they might encounter violent death in the shape of a young girl?'

The RAF has been associated with a tactic that I have described as the use of femininity as camouflage: individuals or groups made effective use of feminine accessories (e.g., dresses, make up, hand bags, etc.) and stereotypes (e.g., passivity, submissiveness, peacefulness) to prepare or carry out violent attacks. While the murder of Jürgen Ponto brought this tactic to the media's attention in Germany, the attack was of course neither the first nor the last use of femininity as camouflage in the history of terrorism. It is possible to trace this tactic back to the Russian Anarchists' 'propaganda of the deed' in the late 19th century, and it has been used in a range of political and cultural contexts including the Algerian Civil War and suicide attacks by the Islamist extremist group Boko Haram in Nigeria.

Although the suggestion that every citizen should fear death in the shape of a young girl was clearly exaggerated, research has shown that almost half of the RAF members and almost all of the group's leading ideologists were women. The best known examples are Ulrike Meinhof (1934-1976), Gudrun Ensslin (1940-1977), and Brigitte Mohnhaupt (1949-present). This is striking, because there were hardly any women in leading positions in West Germany at that point.

Like their male counterparts, women have historically participated in armed political struggles for a range of reasons, and they have identified with different theoretical and ideological positions. Whilst wanting to be equal to their male comrades in every regard, women in the RAF distanced themselves from feminism. Other women in the militant left in West Germany, by contrast, identified with the aims and ethics of the women's movement. The Red Zora, for example, was a self-declared women's guerrilla group with an explicitly feminist agenda that formed in the mid-1970s and carried out dozens of arson attacks and bombings, most of which took place in the 1980s.

The RAF and the Red Zora carried out their last attacks in the early 1990s. By then, the political landscape and the gender dynamics in Germany had changed significantly: although still greatly outnumbered by men, women were represented in leading positions in education, politics and industry. Recent years have seen further steps towards gender equality. In 2001, the first 244 female soldiers joined the Federal Armed Forces, and today there are more than 20,000 women in the army. In 2005, Angela Merkel became the first female Chancellor, and has remained in power since. These developments raise an important question: have women in the RAF and other terrorist organisations helped to pave the way for women in other spheres of society?

Recent studies have come to different conclusions regarding this question. Some have argued that female political violence has exposed and challenged the repressive gender regime in post-war Germany. Others have disagreed, acknowledging that the RAF put into practise a kind of subconscious feminism but that this violent activism jeopardised feminist aims. While more studies on this subject are needed – especially on a comparative level – my research shows that female political violence can, but does not necessarily, have a feminist background or agenda, and it is certainly no guarantee for a gender revolution.

Dr Katharina Karcher is a Research Fellow in the Faculty of Modern and Medieval Languages at the University of Cambridge.

BENJAMIN LEE

UNDERSTANDING THE FAR-RIGHT LANDSCAPE

Benjamin Lee demonstrates that, although the vast majority of far-right activists are non-violent, far-right activism has security implications in the UK and globally.

Developing a coherent picture of the far-right is becoming harder. Although most people have a rough understanding of far-right activism as highly nationalistic, nativist, xenophobic, and in some cases violent, objective definitions of the far-right are hard to come by.

The label ‘far-right’ is best thought of as an ideological container for a range of groups and actors. It has been applied to groups as diverse as revolutionary neo-Nazi groups, and right-wing populist parties with parliamentary representation.

In part, this confusion is explained by the inconsistent use of terminology. Descriptions like ‘extreme’, for example, are often used to describe groups outside of formal democratic politics, while those contesting elections on the far-right are more often considered ‘radical’. Terms like ‘Nazi’ and ‘fascist’, tend to have more specific meanings, but these are often misused in highly charged political spaces. The adoption of the label ‘populist’ to describe anti-immigration and nationalistic right-wing parties is, according to some, an attempt to paint over explicitly fascist legacies.

Added to the politicised and highly contested language surrounding the far-right is the increasingly complex organisational picture. Readily adopting new communications channels, the far-right has become a series of networks with traditional hierarchical organisations growing rarer. Terrorists, like Anders Breivik, are free to access material from a range of positions on offer, cobbling their own ideologies together without the need for a centralised doctrine. As shown by the English Defence League, concepts such as membership are less important. The apparent mismatch between online support and participation in direct action also calls into question the commitment of many far-right activists.

The vast majority of far-right activists are non-violent, but they are an important consideration in security analysis. Acts of mass-casualty terrorism from the far-right, such as the 2011 attacks in Norway that killed 77, are rare but unpredictable. The far-right has also been influential in several acts of smaller scale violence, including the murder of Labour MP Jo Cox in 2016, and the attempted murder of Dr Sarandev Bhambra in 2015.

Far-right groups and activists can also be the targets of violence. In 2015, two gunmen were killed in their attempt to attack a ‘Draw Mohammed’ contest in Garland, Texas, USA. In 2012, an attempted attack on an English Defence League rally in Dewsbury was uncovered by British police.

Although the relationship between hate crime and politics is difficult to unpick, organisations like Tell Mama and the Community Security Trust have argued that the far-right is linked to hate crime attacks. Far-right activism also comes at a cost to public order. Where mass public demonstrations are used as a tactic, the costs of policing and associated violence (often involving anti-fascists) lead to significant economic and social harms. Finally, far-right activism supports narratives of other extreme groups, such as Islamic State, that seek to convince sections of the population that they cannot live peacefully in the UK, or the West more generally. Far-right activism that seeks to demonise minority groups such as Muslims potentially contributes to wider narratives of polarisation and resulting security threats.

Written by Dr Benjamin Lee, CREST has produced a guide to the far-right landscape. You can download it for free from the CREST website. CREST produces a range of informative, accessible guides on a wide variety of topics. Download them at www.crestresearch.ac.uk/resources

CREST GUIDE:
UNDERSTANDING THE FAR-RIGHT LANDSCAPE

[illegible]

“Although the vast majority of far-right activists are non-violent, far-right activism has security implications in the UK and globally.”

OVERVIEW

[illegible]

THE BLUFFERS GUIDE TO NETWORKS

Researchers on networks, and especially social network analysis, use a variety of technical terms to describe the elements and structure of a network. But, what do they actually mean?

NODES

The nodes (also known as 'actors' and 'vertices') are the people or entities that make up the members of the network. They can be individuals, organisations, sub-teams, roles or even pieces of technology. Whatever they are, they are the 'blobs' or 'dots' in a network diagram. So, in the expression "Suspect A provides a tasking to Suspect B" we have two nodes (persons A and B) and a relationship ('provides tasking') that connects the two.

TIE/EDGE

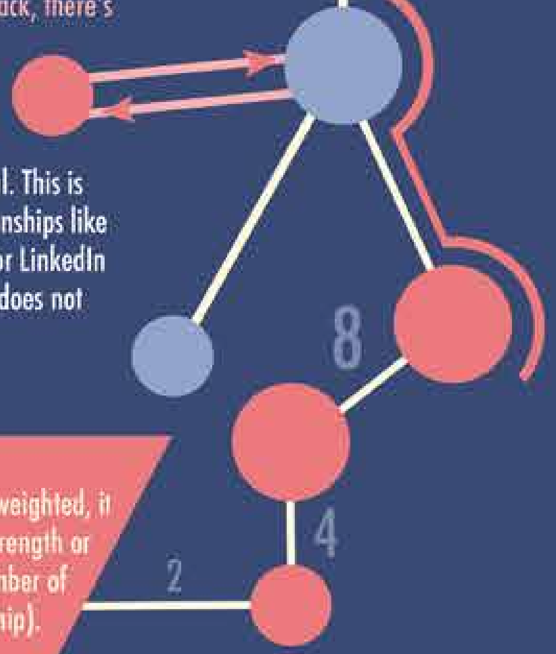
The connections or relationships between nodes are called 'ties' or 'edges'. A tie suggests a connection of some sort between two nodes.

MULTI-DIRECTIONAL TIES

Some ties have arrows showing the direction of a connection. So, if person A sends instructions to person B, that tie would have an arrow pointing from A to B. If B returns something back, there's another tie, with an arrow in the opposite direction.

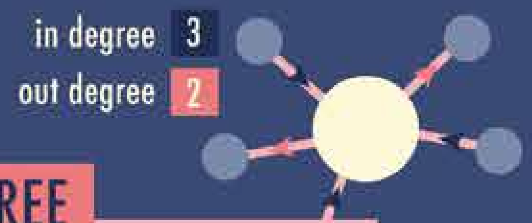
UNI-DIRECTIONAL TIES

If there's no direction in a tie then it is uni-directional. This is shown with a single link. It would be used for relationships like kinship, or for reciprocal connections like Facebook or LinkedIn contacts (unlike Twitter, where A can follow B, but B does not need to follow A).



WEIGHTS

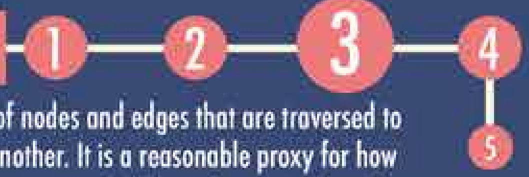
A tie can be weighted or unweighted. If it's weighted, it has a numerical value that represents the strength or frequency of a connection (for instance, number of messages exchanged, closeness of relationship).



NODE DEGREE

Simply the number of connections coming into a node (in-degree) and out of a node (out degree). Degree centrality is the number of connections a node has – it is a simple measure of influence, but having more connections doesn't always mean someone is more influential.

DISTANCE



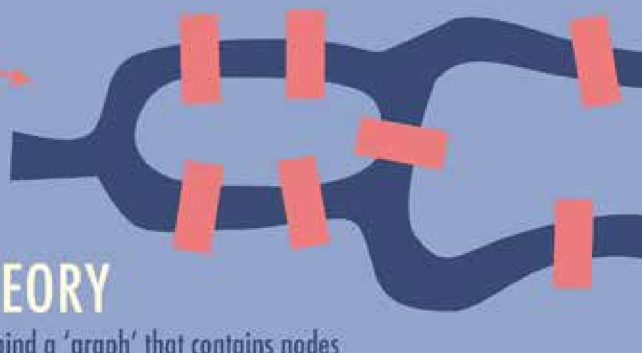
'Distance' is the number of nodes and edges that are traversed to reach from one point to another. It is a reasonable proxy for how much potential influence a person might have in a network – if they have to cover a considerable distance to reach most other nodes, their reach and influence is likely to be less than a person with easier access to the rest of the network.

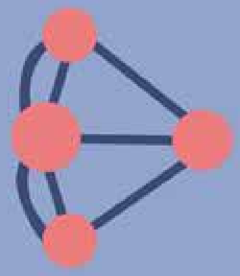
PATH

If you imagine a network made up of nodes and edges, the 'path' is the route between any two nodes. So, If Ted is connected to Sam who connects to Georgina, then a path would be from Ted > Sam > Georgina.

BRIDGES OF KÖNIGSBERG

The original problem, how to cross the bridges once and only once, that led mathematician Euler to publish the first paper on graph theory in 1736.



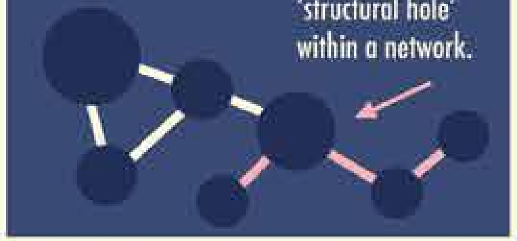


GRAPH THEORY

The mathematics behind a 'graph' that contains nodes ('vertices') and ties ('edges'). Graph theory describes how a network is drawn, as well as how the structure of the network can be expressed mathematically.

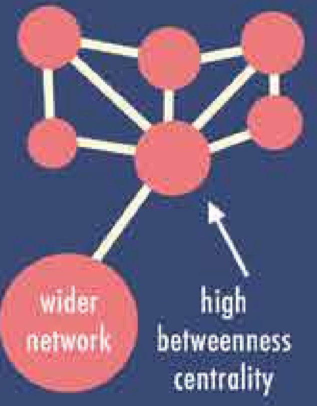
BRIDGE / BOUNDARY SPANNER

A node that connects up two or more nodes / sub-sets of nodes that would be disconnected otherwise. A lack of a bridge creates a 'structural hole' within a network.



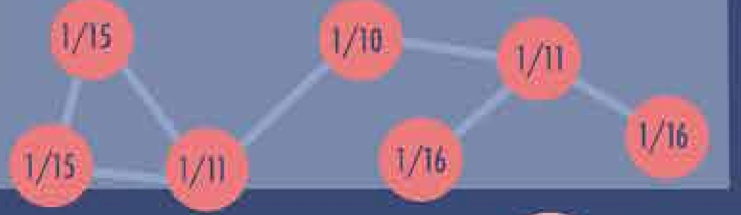
BETWEENNESS CENTRALITY

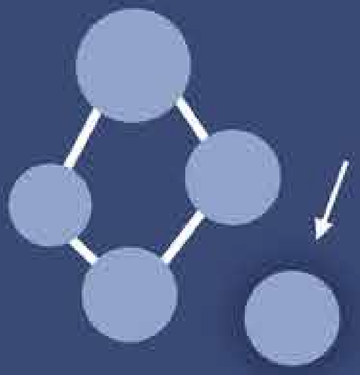
A measure that expresses the likelihood of a node being a 'bridge' or 'boundary spanner'. For instance, if a terrorist cell has six closely connected members, but only one has connection to the wider network, that one person would score higher in betweenness centrality.



CLOSENESS CENTRALITY

A score that expresses the average distance of a single point to reach all other points in a network (or graph). A higher score means that the node is 'closer' to the rest of the network – meaning that they have better sight of the overall network.

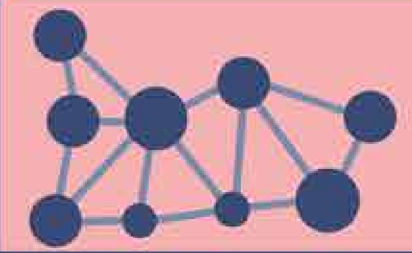




STRUCTURAL HOLE

An area within a network where there are no ties between nodes. Structural holes can be exploited by 'boundary spanners' (or entrepreneurs) to create value by identifying complementary ideas or products and connecting them.

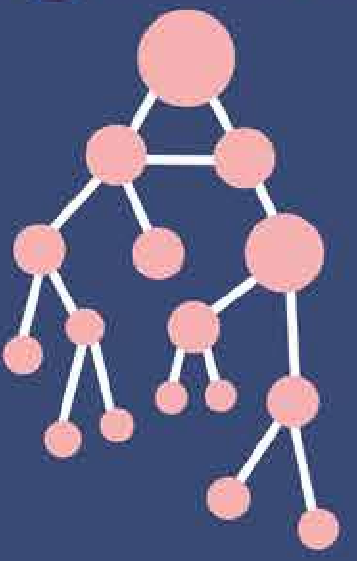
DENSITY



The degree to which all nodes are connected to each other. A densely connected network will be more resilient to the removal of nodes (and their edges) since other routes exist to connect up.

CASCADES

The term used to describe how information spreads across a network (e.g., news, rumour, pattern of behaviour). The 'seed' node is the originator of the information, and if their connections propagate to their connections (or copy the behaviour), and then their contacts do the same, then a 'cascade' has begun.



CREST
CENTRE FOR RESEARCH AND EVIDENCE ON SECURITY THREATS

CREST Security Review provides a gateway to the very best knowledge and expertise. Its articles translate academic jargon to 'so what' answers and illustrate how behavioural and social science can be used effectively in everyday scenarios.

THE CENTRE FOR RESEARCH AND EVIDENCE ON SECURITY THREATS

CSR is produced by the Centre for Research and Evidence on Security Threats (CREST). CREST is funded by the UK's security and intelligence agencies to identify and produce social science that enhances their understanding of security threats and capacity to counter them. CREST also receives funding from its six founding partners (the universities of Bath, Birmingham, Cranfield, Lancaster, Portsmouth and West of England). Its funding is administered by the Economic and Social Research Council (ESRC Award ES/N009614/1), one of seven UK Research Councils, which direct taxpayers' money towards academic research and training. The ESRC ensures the academic independence and rigour of CREST's work.

CREST has established a growing international network of over 100 researchers, commissioned research in priority areas, and begun to tackle some of the field's most pressing questions.

"There really is some impressive work going on. Yet, all that effort is irrelevant if practitioners, policy-makers, and other stakeholders do not get to hear about it. *CREST Security Review* is one way we will keep stakeholders informed not only on what CREST is doing, but also on the best research from around the world."
Professor Paul Taylor, CREST Director

For more information on CREST and its work visit
http://www.crestresearch.ac.uk/resources/ and follow us on twitter **@crest_research**

Lancaster University   UNIVERSITY OF BIRMINGHAM   University of Portsmouth

UNIVERSITY OF BATH   Cranfield University   UWE BRISTOL University of the West of England   E·S·R·C ECONOMIC & SOCIAL RESEARCH COUNCIL