SIMON HENDERSON

THE TRADE OF THE TRICKS:
HOW PRINCIPLES OF MAGIC CAN CONTRIBUTE TO NATIONAL SECURITY

The goal of magic is to engage and entertain an audience through the creation of a false, apparently impossible reality. Accordingly, magicians employ a rich repertoire of strategies to influence and fool an audience's understanding about the state of the world.

This includes methods for manipulating their attention – including where the audience is looking and what they are listening to; perception – including what the audience is seeing and hearing; sensemaking – what the audience understands about what is happening and what they decide to do about it; expectations – what the audience thinks will happen next; and emotion – how the audience feels about what they are experiencing. Importantly, magicians use these strategies to influence and deceive their audiences without the need to lie.

Magic is sometimes referred to as 'mind hacking', and its underlying principles and methods have the potential to support both offensive and defensive security applications. The capability to influence a subject of interest's understanding about the world and their resultant behaviour can contribute to a wide variety of security applications, including the deterrence of state-based threats, disruption of terrorist activity and enhancement of cyber security.

MISDIRECTION

For example, the likelihood of the public noticing, attending to and correctly making sense of safety and security notices could be increased by exploiting principles of conspicuity amplification used in magic. Many magic effects rely upon an audience actively noticing and paying attention to certain features; indeed, the fundamental principle of misdirection actually involves influencing the direction of spectators' attention.

Magicians exploit conspicuity to attract or seduce their spectators' attention through the amplification of properties including intensity, size, movement, contrast, position, novelty, repetition, and absence. A glamorous assistant wearing a brightly coloured outfit who walks on-stage from the wings carrying a golden envelope is likely to attract the attention of the audience, as they will be moving, wearing a colour that contrasts with the background of the stage, and holding a novel item. As the audience cannot direct its attention to two locations simultaneously, this event misdirects the spectator's attention away from the magician, and creates the perfect moment (referred to by magicians as an 'off-beat') for the magician to switch the deck of cards they are holding for another (stacked) deck in their pocket.

In a security context, principles of conspicuity and misdirection could be employed to disrupt hostile surveillance of sensitive logistics and deployment activities, seducing an attacker's attention away from the real transportation of sensitive equipments and materials, onto more conspicuous, yet simulated, transportation activities.

HAVERSACK RUSES

The probability of hostile actors detecting covertly deployed surveillance assets could also be reduced, both by attenuating their conspicuity, and via the application of perceptual manipulation strategies. Parts of the critical national infrastructure could, for example, be blended with their background, made less obvious or interesting, or be modified to resemble other things.

Strategies used by magicians for manipulating spectators' perception include masking – putting something in-between the spectator and the object to be hidden; blending – making the thing to be hidden look like its background; repackaging – wrapping the object in other signifier cues that change its appearance to resemble a different object; and dazzling – breaking up the object's pattern of cues that are used for identification.

Attackers could be lured away from real assets towards false, low value decoys, and high-value assets could be hidden amongst a sea of indistinguishable low-cost simulations. The perceived footprint, conspicuity and potency of protective measures could be amplified, and cyber attackers, for example, could be lured into spending time and resources attacking the wrong targets, erroneously believing that they have been successful, and unintentionally disclosing their capabilities and strategies.

Some magic effects allow a spectator to think that they have surreptitiously acquired useful information when they have not. This is a stratagem known as the 'Haversack Ruse', named after an apocryphal event that supposedly occurred during the 1917 Sinai and Palestine Campaign, when Colonel Richard Meinertzhagen let a haversack containing false British battle plans fall into Ottoman military hands, thereby bringing about British victory in the Battle of Beersheba and Gaza.

In magic, use of the Haversack Ruse might involve the spectator 'accidentally' catching a glimpse of the face of a card as it is placed by the magician onto the table. During the act of placing the card, the magician will execute a one-handed change that exchanges the glimpsed card for another.

In the cyber security domain, honey encryption similarly allows a cyber attacker to believe that they have surreptitiously acquired useful information when they have not. A honey-encrypted file (containing, for example, credit card details) will resist brute-force password generation attacks by appearing to resolve into plaintext during decryption, when in fact the critical data remains encrypted as ciphertext.

COUNTER-INFLUENCE

The strategies used by magicians to influence people are scalable from individuals to collectives, and work by exploiting fundamental tendencies in human psychology and physiology. This means that they can be employed to influence large multi-cultural and heterogeneous audiences without any requirement to first collect and analyse intelligence about them.

Many of the strategies that enable magic can be applied readily within the cyber domain, where hostile actors (and their software proxies) remain just as susceptible to being influenced and deceived as they are in other venues of human activity, and where many of the inherent risks also create new opportunities.

The potential to enhance influence and deception gives rise to a reciprocal and critical need for counter-influence and counter-deception. Influence approaches from magic can be inverted, that is, to support the detection and management of adversarial influence and deception.

Analysis using an understanding of magic can inform the detection, identification and unpicking of the methods by which hostile capabilities and threats are obfuscated, false intent revealed and conveyed, misattribution traps set, false-flags raised, and causes divorced from effects. The value of magicians in a 'poacher turned gamekeeper' role also has precedence, wherein such practitioners of influence and deception are often well placed to detect and explain it when it is used by others.

LIMITATIONS

Despite the potential for the principles of magic to contribute to national security, it is important that stakeholders and researchers remain aware of magic's limitations. The goal of performance magic is ultimately to influence an audience's sensemaking, and not its behaviour; and magic always necessitates a reveal, thereby signalling to the audience that they have been deceived. In many security applications, influence and deception is only effective if it is never suspected, let alone detected by an attacker.

Magic is intended to fool a largely passive audience that is ignorant of the methods employed, and magicians rarely need to account for risks to life, property, relationships and ethics in the design of their effects. Professional magicians also benefit by exaggerating their influence and deception skills when the tools of their trade may in fact be far more prosaic. Finally, publicity is the lifeblood of professional magicians, a disposition incompatible with most applications of security.

EXPLOITING MAGIC TO ENHANCE NATIONAL SECURITY

The field of magic possesses a rich hoard of esoteric, utilitarian, and, to-date, largely untapped knowledge about influence and deception that could make a positive contribution across multiple security domains. Three ways in which this might be achieved are outlined.

First, knowledge from the field of performance magic should be better incorporated into ongoing research about how individuals and organisations make sense of the world, and how this activity can be manipulated by others. Second, principles of magic should be exploited to enhance operational training for those security, intelligence and counter-terrorism staffs that would benefit from enhanced 'sneaky thinking' and counter-deception skills. Third, design methods used by magicians to construct magic effects should be exploited in the development of enhanced protective and cyber security capabilities.

....

Simon Henderson is a director at Artifice Ltd, a small research and training company that helps select government communities, elite sports teams, and specialised business units to become better at sneaky thinking, enabling them to realise new forms of competitive advantage in adversarial settings. Simon is a lifelong student of magic and has created and published a number of original effects