

## Chapter 78

# Building National Resilience in the Digital Era of Violent Extremism: Systems and People

**Jethro Tan**

*Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore*

**Yingmin Wang**

*Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore*

**Danielle Gomes**

*Home Team Behavioural Sciences Centre, Ministry of Home Affairs, Singapore*

### **ABSTRACT**

*The threat of violent extremism in the Internet age has undoubtedly become one important focus of research, policy, and government bodies all over the world. Understandably, many resources have been invested into counter violent extremism efforts, such as the identification of possible radicalised individuals, and understanding the psychology behind violent extremism. These methods adopt a resistance stance and attempt to prevent violent extremism. However, this chapter argues that resilience is equally, if not more important given the unpredictable nature of violent extremism. The first part examines ‘systems’ within a nation such as critical infrastructure and how concepts such as ‘resilient-by-design’ can be incorporated to ensure continuity in times of attacks. The second part will explore ‘person’ factors of crisis communication, cohesion, and social capital, and how these factors can afford a cohesive society that can overcome the cracks in social order and harmony often caused by violent extremism.*

## **INTRODUCTION**

Countering violent extremism has become a cornerstone concern of national security, especially after the notorious attack on the World Trade Centre in the United States on September 11, 2001. Subsequently, the ‘war on terror’ has hardly paused, with no signs of abating in the near future. Such strategies had involved security measures (e.g., surveillance) and military interventions on violent extremist groups (Global Policy Forum, n.d). Evidently, relying on the strategy of resisting against violent extremists is simply inadequate. Successful attacks in cities such as the London underground bombings of 2005, the Charlie Hebdo shooting in Paris, and hostage situation in Sydney, among many other attacks all over the world, illustrate the complexity behind countering violent extremism. Indeed, nations are often reminded of the threat posed by violent extremism despite increased efforts to keep violent extremists at bay.

More recently, the presence of the Islamic State in Iraq and Syria (ISIS) on social media, the concerns of the influx of foreign fighters to Iraq and Syria, and the dissemination of videos of brutal murders of innocent people are some manifestation of online violent extremism. The strategic use of technology and the Internet has brought forth an unprecedented age of violent extremism and radicalisation through the digital space. As such, the threat of violent extremism in the Internet age has undoubtedly become one important focus for researchers, policymakers, and government bodies across the world. This goes to show that the threat of violent extremism is an evolving one, often pitting law enforcement and policymakers against the violent extremists who are constantly stepping up their game.

## **VIOLENT EXTREMISM IN THE DIGITAL ERA**

The threat of violent extremism has become more potent in the digital era. While the advent of the Internet and subsequent info-communication technologies has brought along innovative solutions to life, it also brings about critical security concerns (Hussain & Saltman, 2014; Weimann, 2004). This implies that radical ideologies are capable of spreading at a speed previously unseen before. Cases of lone-wolf radicalisation (e.g., Roshonara Choudhry) illustrate the effectiveness of the Internet as a medium to propagate radical ideologies. Calls for attacks by radical propagators have also been found to cause critical disturbance to the functioning of the nation and compromise the safety of citizens (e.g., Sydney Siege). More importantly, these case examples raised indicate that violent extremism initiated and propagated online have the potential to cause significant harm in the offline space.

Understandably, many resources have been invested into countering violent extremism, such as the identification of possible radicalised individuals, understanding the psychology of violent extremists, or even technological warfare (e.g., drone attacks). These methods attempt to circumvent the consequences of violent extremism, which evidently will cause chaos in the highly connected world we live in. These counter violent extremism efforts adopt a ‘resistance’ stance (Longstaff, Armstrong, Perrin, Parker, & Hidek, 2010; Ng, 2011), and are essential to provide safety to the people and ensure growth of the economy.

However, preventive measures against violent extremism, while shown to be practical (Qatar International Academy for Security Studies, 2010), should not be the only measure taken against violent extremism. It is equally imperative to entertain the thought of how to respond to a violent extremist attack that comes into fruition. In doing so, researchers, policymakers, and government bodies can then implement strategies to enhance the ability of the nation to bounce back from the attack, and ensure

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:  
[www.igi-global.com/chapter/building-national-resilience-in-the-digital-era-of-violent-extremism/251495](http://www.igi-global.com/chapter/building-national-resilience-in-the-digital-era-of-violent-extremism/251495)

## Related Content

---

### The Triumph of Fear: Connecting the Dots about Whistleblowers and Surveillance

David L. Altheide (2014). *International Journal of Cyber Warfare and Terrorism* (pp. 1-7).

[www.irma-international.org/article/the-triumph-of-fear/110977](http://www.irma-international.org/article/the-triumph-of-fear/110977)

### The Role of Human Operators' Suspicion in the Detection of Cyber Attacks

Leanne Hirshfield, Philip Bobko, Alex J. Barelka, Mark R. Costa, Gregory J. Funke, Vincent F. Mancuso, Victor Finomore and Benjamin A. Knott (2015). *International Journal of Cyber Warfare and Terrorism* (pp. 28-44).

[www.irma-international.org/article/the-role-of-human-operators-suspicion-in-the-detection-of-cyber-attacks/141225](http://www.irma-international.org/article/the-role-of-human-operators-suspicion-in-the-detection-of-cyber-attacks/141225)

### Bouncing Techniques

Stéphane Coulondre (2007). *Cyber Warfare and Cyber Terrorism* (pp. 392-396).

[www.irma-international.org/chapter/bouncing-techniques/7477](http://www.irma-international.org/chapter/bouncing-techniques/7477)

### Knowledge Management, Terrorism, and Cyber Terrorism

Gil Ariely (2007). *Cyber Warfare and Cyber Terrorism* (pp. 7-16).

[www.irma-international.org/chapter/knowledge-management-terrorism-cyber-terrorism/7434](http://www.irma-international.org/chapter/knowledge-management-terrorism-cyber-terrorism/7434)

### Malware: Specialized Trojan Horse

Stefan Kiltz, Andreas Lang and Jana Dittmann (2007). *Cyber Warfare and Cyber Terrorism* (pp. 154-160).

[www.irma-international.org/chapter/malware-specialized-trojan-horse/7452](http://www.irma-international.org/chapter/malware-specialized-trojan-horse/7452)