

21st century border security

an address to the Institute on 30 May 2017 by

John Coyne

Australian Strategic Policy Institute¹



In recent years, the ‘all-hazards’ approach has broadened the scope of national security so as to embrace transnational migration, cyber-crime and terrorism. In response to this new thinking, some of the most basic assumptions about geographically-defined national borders are dramatically changing. In these shifting sands, strategists are being challenged to think beyond traditional ‘detect and disrupt’ border security operations. Instead, they are encouraged to perceive the border as a national security vector. In responding to the challenge of 21st century border security, countries are being polarised between militarisation and securitisation methodologies. Nevertheless, to be effective, a border security strategy must be integrated within a whole-of-government national and domestic security strategy.

Key words: border security; 21st century borders; types of threat; Australia; China; Russia; transnational migration; cyber-crime; terrorism; border security strategies.

Events like Russia’s hybrid war in the Ukraine, the 2015 European migration crisis, the chaos in Syria, the troubles in the South China Sea, the Manchester bombing, the recent ‘Wannacry’ global cyber-attack, and the London Bridge attack, all serve to illustrate how the scope of national security threats has broadened. Moreover, these events have ensured that domestic, border and national security are key policy at the forefront of the electorates’ minds in various western liberal democracies, including Australia (Jones and Johnson 2016).

Traditional conceptions of national security have focused mainly on the direct kinetic threat posed to a state by another sovereign state (Price 2001). More contemporary national security thinking focuses on a much broader scope:

- societal – new sources of information and communication mean new channels for empowering dangerous, destructive ideologies that threaten social cohesion;
- environmental – climate change, disease and environmental degradation threaten food and water security, health and economic productivity, and create immigration pressures;
- economic – demographic and technological changes, coupled with other factors like resource scarcity, threaten economies and standard of living, adding to societal pressures; and
- political security – societal, environmental and economic pressures feed destabilizing narratives and movements, and new technologies allow these to proliferate faster than traditional political processes can counter them.

The traditional ways of thinking about borders are being challenged by an increasingly globalised, connected and interdependent world. Rather than just

being a line on a map, the border is now elastic, virtual, and socially and psychologically constructed. With all of this change has come a need for an equally dynamic revolution in border security strategy and policy thinking.

Australia’s lack of a shared land border make understanding concepts such as ‘*the border*’ and ‘*border security*’ abstract in nature. Consequently, many public commentators take a default position that our coastline is our border and that border security involves merely police, security guards and immigration or customs officials patrolling airports and seaports. These conceptual frameworks, however, are limited, given the nature of 21st century borders.

The Border as a Security Vector

The assessment of the threat and risk posed by individuals crossing the border is an increasingly problematic proposition for border security officials. The process of moving through the border can change a threat source’s capability to undertake illegal, disruptive or otherwise deviant activities. Consequently, transition through the border can influence the likelihood that a national or domestic security risk might be realised. When it comes to the assessment of risk and threat posed by an individual, borders are a transition point for changes in the nature and scope of risk or threat. Arguably then, the national and domestic security challenges at borders do not relate to migrants or transactions *per se*, but to the assessment of the likelihood that national and domestic security risks will be realised.

Hybrid Warfare and Border Security

While proxy wars still rage across the globe, and Russian, American, English, French and Australian expeditionary operations continue to evolve, there should be little doubt that hybrid warfare strategies are becoming increasingly prevalent. Fishing fleets operating illegally, cyber-attacks, deniable public information

¹Email: johncoyne@aspi.org.au

campaigns, and hate preachers can no longer be categorised simply as border, domestic, criminal or national security issues. Instead, these kinds of activities must be analysed to consider whether they are elements of a broader threat strategy. For this reason, amongst more general threat challenges, border security is becoming an increasingly important component of the national security apparatus. Responding to this new dimension in state and non-state strategies, countries need whole-of-government strategies that break down the silos of traditional border, law enforcement, domestic security and national security strategies.

China's militarised fishing fleet serves as a regional example of this new challenge in action. China's distant water fishing fleet is now the world's largest, and for the most part state owned. With an ongoing global food protein shortage, this fishing fleet provides the Chinese with access to valuable protein. On the other hand, the fishing fleet also contributes to the achievement of China's grand strategy which is more focused on geopolitical aspirations than krill. Through its constant intrusions into the exclusive economic zone² of ASEAN³ member states, the Chinese fishing fleet is able to push sovereignty 'red lines' and in the process create new norms of regional behaviour. China also has enhanced the roles of both its coast guard and its naval paramilitary force in these endeavours. The strategy presents a particularly difficult national security challenge. Military responses to the Chinese fishing fleets' operations are quickly viewed as escalatory. As such, this maritime border issue quickly escalates into a national security issue.

Likewise, analysis of Russia's actions in the Ukraine over the last five years quickly reveals the important relationships between border, domestic and national security needed to defeat hybrid warfare. Russia penetrated Ukraine's borders with political influence as soon as the country became independent. Pro-Russian factions were formed and sustained by Moscow to exploit weakness in the new Ukrainian government. The internet has no shortage of photographs and videos showing armed men in Crimea who look like members of the Russian military. While Russia denies it, it would seem these 'little green men', along with such deniable activities as cyber-attacks on power stations and mis-information, are part of a wider hybrid campaign that represents an existential threat to the Ukrainian government. In protecting itself, Ukrainian border security needs to be integrated into the country's overarching national security strategy for dealing with Russia.

Old Threats but New Challenges

The globalised operating context of sovereign states, ensures that non-state border security threats affect

national security. With this perspective, the understanding of the threats posed by irregular migration and transnational and serious organised crime (TSOC) can be enhanced through whole-of-government co-operation in intelligence sharing and policy co-ordination. The TSOC threat has become a focal point for a range of private-sector and public-sector stakeholders, but there appears to be little evidence of strategy integration.

At the top of the list of pervasive and persistent non-state border threats is TSOC. The line between TSOC, some sovereign states, and politically-motivated groups, is increasingly blurred. The increasing scope of TSOC activity has been accompanied by an increase in the complexity of TSOC structures and activities. From groups that have manipulated stock exchanges to those that have more recently shut down the British National Health care service through a cyber-attack, TSOC is increasingly being perceived as a national security threat.

TSOC decision-making is supported by all manner of open-source information, including information on government strategies and operations. These TSOC networks are then able to rapidly change operations or activities and take immediate action when an opportunity or unacceptable risk arises. Alarming, the TSOC operating models allow for the rapid purchase and employment of new technology at a rate that far exceeds that available to government – and this brings with it significant challenges.

The border risks are further broadened by issues such as counter-proliferation, biohazards and trade-based money laundering. Many of these are interconnected and require sophisticated responses, as equally committed to creating a strong economy and a cohesive society, as to undertaking enforcement and regulatory compliance. This is particularly the case when it comes to cyber borders.

One of the most controversial issues relating to the cyber border is encryption. Encryption is a central contributor to the health of the global economy and business competition. The encryption trend cannot be stopped, and industry often is unable to 'hand over the keys' to their encryption, nor build backdoors into their systems. Encryption is rightfully here to stay and will continue to rapidly improve, so governments must invest in the research and development of technological solutions that are legal, affordable and practical. Then again, this approach will not fully resolve the encryption challenge.

Internal or domestic security has also emerged as a critical aspect of border security, because of those people who have travelled legally to Australia to undertake either illegal or disruptive acts. In this new strategic environment, it is not easy to identify whether these individuals are linked with TSOC or violent non-state actors, or are part of a wider strategy to exert influence.

Border security strategy

A specific, and universally accepted, definition of

²An exclusive economic zone (EEZ) is a sea zone prescribed by the United Nations Convention on the Law of the Sea over which a state has special rights regarding the exploration and use of marine resources, including energy production from water and wind. It stretches from the baseline out to 200 nautical miles from its coast.

³Association of South East Asian Nations

border security is yet to be developed. Given the integrated nature of economies and communities, it may be that a nation can never completely 'secure its borders' in the 21st Century. This is certainly the case if a definitive guarantee of security is expected from the state, at the same time as maintaining the economically-necessary flow of people, goods and value across the national border. Even though defining border security in today's globalised and high-tech world is difficult, citizens expect that their governments can prevent harms or threats from entering borders. In an age when diverse non-traditional national security threats affect the day-to-day lives of citizens, there should be little surprise that public interest in border security is increasing across the world.

Interconnectedness and integration are key dynamics influencing economic growth for nation-states. While border security is becoming an increasingly important national security imperative, contemporary economic policy seeks to accelerate border reform so that barriers and burdens on trade and travel are removed. This creates a potential conflict space between economic reformers and security professionals over border management.

Physical borders still exist; and their protection in terms of maintaining national sovereignty remain a foundational key-stone for national security. Conversely, in the face of 21st century borders, there is a need for substantial changes to how nation-states think of border security. Already, traditional administrative practices at Australia's border are being aligned with enforcement models, the net effect of which is the securitisation of the border. This is a start point. These processes now need to be integrated into a broader strategy.

Reducing the concept of border security to a discussion about balancing between securing and not-securing national borders is too simplistic. Similarly, reducing the border security challenge to a spectrum limits decision-makers' opportunities to develop innovative strategies that can be assessed on the basis of their merits, including opportunity costs. Arguably then, border security may be more akin to an aspirational goal than to an end state. If that is the case, the border security question should then involve a detailed analysis of national risks. More specifically, the challenge could be recast into a question about what level of residual border security risk governments should accept.

In Australia, the strategy response to the border security challenge has been to create depth in the border security policy framework through a border security continuum model. The continuum model elongates the border to allow for decisions, including those about the disruption of potential threats and risks, well before the physical border. Then again, this approach still does not always give sufficient consideration to the transmission and transition impacts on threat and risk from border transactions. Nor does this model ensure the integration of border security strategy and operations with other government actions.

One particularly helpful way of conceiving border security's complex array of intertwined control and

mitigation national security capabilities is as a 'system of systems'. In responding and shaping responses, border security strategists fine-tune the various systems within the border and national security system, or ecosystem, to achieve strategic outcomes. This way of thinking highlights the high-level challenges of integrating border security in national security strategy.

The risks and threats posed by the 21st century transnational and serious organised crime and terrorism are amorphous and adaptive, which in turn supports the development of a more agile border security capability. The border security challenge is not just concerned with policy-setting mechanisms. There are also continual challenges in operationalising policy decisions, often due to a lack of organisational agility in border security agencies. These agencies are more accustomed to the delivery of services or processes. In border security practice, agencies should be able to rapidly deploy capabilities in response to evolving threats, risks or opportunities – the kind of operational and organisational agility that would allow border agencies to deal with evolving changes in either security or economic concerns.

The increasingly transnational dimensions of non-state threats ensures that the difference between domestic and national security issues is no longer as clear as it once was. Europe's experience with the 2015 mass-migration crisis illustrated that those with responsibility for border security face impossible expectations that they can manage extraordinary challenges without the benefit of additional resources and powers. Knowing when an issue is likely to become an extraordinary policy challenge is difficult, and reliant on sensitive interdepartmental intelligence sharing. In this landscape, governments should strive unilaterally and multilaterally to improve inter-institutional communication and inter-service co-operation.

Border security agencies cannot be expected, on their own, to disrupt or mitigate all border risk or threats all of the time. Arguably, border, national and domestic security policymakers need to work together to identify the most efficient and effective strategies to disrupt threats and risks, whatever they may be. This decision-making must also be underpinned by a comprehensive understanding of threats and risks. With such an understanding, policymakers can selectively apply measures if, or when, needed while still achieving strategic outcomes. Collaborative and integrated border security strategies will ensure that a nation's resources are focused on managing risks and disrupting threats, rather than on building walls. But this needs to be supported by a sensitive whole-of-government intelligence fusion capability.

To date, border security philosophies and strategies have, for the most part, had a one dimensional focus on keeping things and people from entering one's borders. In the face of terrorism, governments have increasingly sought to protect their communities from the border inwards. The militarisation of border security is particularly evident in the United States, where the

Department of Homeland Security uses an approach that is somewhat reminiscent of the walled frontiers of the Cold War. In contrast, both the European Union's Frontex and the United Kingdom's Border Force offer examples of the securitisation model focused on processes and systems. In both cases, performance has been mixed at best, as their strategies remain focused on assessing transactions, and not on managing risk. Yet, border transactions are already so frequent that simplistic responses – such as opening a few extra migration desks at the airport, buying a new x-ray machine for goods or building a new wall – do not really work. To manage border security risks, bureaucrats need new strategies more than new technology, better barriers or more staff.

Conclusion

There has been, and continues to be, irreversible and significant changes to the business of border security. Nevertheless, our strategies, for the most part, have remained static and linear. Discussions of border security innovation are often limited to debates on new walls or biometric advances, not strategy. Unsurprisingly, industry representatives present arguments that some new wall, biometric concept or surveillance platform will 'fix' or ameliorate the border security problem, but those products do not make a strategy.

Border security involves substantially more than building bigger or better security measures. Twenty-first century borders demand the development of not just new technologies, but innovation in border security doctrine, strategies and tactics. Border security must be integrated into whole-of-government strategy. It should involve an array of activities focused on facilitation, revenue collection, regulation and control – all related to the

seamless movement of people and goods across borders. The need for intelligence-led, risk-based, decision-making has never been more important. The risk that an overly-securitised Australian border will have substantial negative economic impacts is real.

The Author: Dr John Coyne is head of the Border Security Programme at the Australian Strategic Policy Institute (ASPI). He joined ASPI in 2015 from the Australian Federal Police, where he worked on transnational and serious organised crime, national security, and counter-terrorism. Over the last 20 years, he has been an intelligence professional at tactical, operational, and strategic levels across a range of military, regulatory, national security, and law enforcement organisations. He has worked extensively in the ASEAN region on a range of bilateral research projects, recently focusing on enhancing multilateral exchange of information on non-traditional illicit commodity flows. His PhD examined strategic intelligence in law enforcement, targeting transnational and serious organised crime. He has written and published on a range of border security and intelligence issues; and he has been a Winston Churchill Fellow and a Vincent Fairfax Fellow. [Photo of Dr Coyne: ASPI]

References

- Jones, R., and Johnson, C. (2016). Border militarisation and the re-articulation of sovereignty. *Transactions of the Institute of British Geographers* 41 (2), 187 – 200.
- Price, R. (2001). From war fighting to crime fighting: transforming the American national security state. *International Studies Review* 3 (3), 31 – 52.