22 CONCLUSIONS: THREAT ACTORS AND DEMOCRACY IN THE NEW SECURITY ENVIRONMENT

by Graham F. Walker [1]

> *The great struggles of the twentieth century between liberty and totalitarianism ended with a decisive victory for the forces of freedom - and a single sustainable model for national success: freedom, democracy, and free enterprise …*
> *These values of freedom are right and true for every person, in every society – and the duty of protecting these values against their enemies is the common calling of freedom-loving people across the globe and across the ages.*
> *President George W. Bush* [2]

We now all live in a new security environment: the world *After 9/11*. It is an environment of challenging complexity, not only because of its globalised and interdependent nature but because so many of the rules that once ordered and directed our daily lives have become irrevocably changed and seem no longer applicable to our present circumstances. This new and violent environment leaves us in a position where we, the constituents of democratic states, must *unlearn* much of what we knew about our established political order. We must conduct a comprehensive reappraisal of our social constructs, from the neighbourhood corner store to the international system and across the virtual cyber-networks which now interconnects us all. To survive and progress in this post-9/11 milieu we need to develop new rules, new frameworks of analysis, and fresh perspectives on old problems. Such an undertaking is vital if we are to construct viable systems of governance that transcend the levels of analysis, from the local to the systemic, and for all the world's constituents to interact within satisfactorily.

Constructing such systems and mechanisms of governance along wqith their corresponding order will be a considerable challenge, to say the very least. But the alternative of not striving towards this ideal is infinitely worse, by any measure, than trying and only half-succeeding or constructing something that is less than perfect. The alternative to this agenda of reappraisal was demonstrated with horrifying clarity before the eyes of the entire world on that bright sunny morning of September 11th, 2001. Constructing modern and adaptable systems of governance that transcend the local to the international without leaving any jurisdictional gaps in legitimate authority, or allowing safe havens and zones of corruption for those who follow corrupt or tyrannical agendas, will be *the* task of the Twenty-First Century; there simply is no alternative.

This volume and its contributors represent just such an attempt to advance this process of re-appraisal and progressive development towards successful policy in the new security environment. They have addressed both the challenges posed to democracies by threat actors, terrorists and criminals alike, and even more importantly the means by which democracies respond to those challenges. Identifying a problem and mapping its interrelated components is the first step for legislators in devising policy with which to mitigate that problem. Evaluating the means by which a government *might* respond ensures that a more nuanced and knowledgeable programme is developed and put forth by government, and that 'unintended consequences' are marginalised when practitioners implement those policies. The variety of topics and concepts addressed in this volume are but an overview of the many issues and potential responses that face us as engaged actors in the new security environment.

The objective of this concluding chapter is to establish an increasingly knowledgeable, and more importantly an 'actionable' understanding of the world after 9/11 for both policy makers and the constituents of the democracies they represent. Summarising the contributions to this volume and identifying their implications is more than an aesthetic undertaking because, as stated in the preface to this volume, from a more comprehensive and nuanced knowledge of the threat actor phenomena and the circumstances in which it occurs will come a foundation for better judgement and better policy with which to address the challenges of the post-9/11 security environment. Both the conceptual and case study chapters in both parts of the monograph offer valuable insights into the sources of these new challenges, and suggest some of the best possible means to address those issues without exacerbating already delicate circumstances.

REVIEWING THE CONTRIBUTORS

As David Charters points out in his first contributions to the monograph, the 9/11 attacks served as an epoch-marking event, one which demarcated the culmination of several evolving trends in global political life, such as the end of the Cold War and the growing prominence of globalisation. While al Qaeda's attacks on September 11th were unprecedented, in both the scale of the destruction and in the enormity of the audience reached, dissecting their tactical anatomy also demonstrates that this transformation is not revolutionary in nature but rather evolutionary. Within the context of the new security environment, where non-state actors now have power commensurate with even the most militaristic of states, 9/11 and al Qaeda represent the latest chapter in an ancient struggle: how man fights to govern himself, authoritarianism versus democracy, taken to a higher 'global' level of conflict where everyone is a participant. Although this has the potential to become an existential threat to the current international system, its asymmetric application is not revolutionary nor is its challenge to Western liberal-democratic values without precedent.

Continuing the conceptual discussions of Part One, Phil Williams argues that for democracies this new milieu demands a paradigm shift in our understanding and thinking about security if we are to successfully meet its existential challenges. To achieve this shift means adopting a holistic approach based on a horizontally structured network model. The tenets of this network model will lead to the generation of policies and security structures that will buttress 'order' in the post-Cold War chaos, and affirm the legitimacy of the very authority that provides the stability necessary for the democratic way of life. However, while advocating a fresh perspective on this new security dilemma, he rejects as a chimera the increasingly popular notion of 'convergence' between criminal and terrorist actors. This 'effects based' notion, he contends, mistakenly focuses on the results of 'activity' rather than on the intentions of 'enterprise,' an error that leads analysts to devise ineffectual policies.

Chris Corpora takes a much different perspective on this new security dilemma, discounting the intention of threat actors in favour of examining the net result of their activities. From this standpoint, all illegitimate actors, intentionally or otherwise, operate synergistically towards the common effect of expanding "zones of disorder" through leveraging and expanding their influence against legitimate authorities' jurisdictions. In zero-sum fashion, this expanding corruption detracts from the legitimacy, and consequently the order and stability, of structures and institutions that civil societies must have to practice democracy and provide for the basic needs of their populace. It is this threat, the challenge to legitimacy and representative authority rather than terrorist or criminal enterprises specifically, that authorities need to address when formulating policy.

Thomas Badey contends that in the new security environment religion, specifically fundamentalist sects like *Wahabism* and *Salifist* Islam, are being used as an ideological tool to both justify and motivate people to commit acts of otherwise unconscionable political violence. He concludes empirically that the premise of religion causing violence is a false one, and further that the U.S. policy community has made an enormous error in assuming that it does. This false premise causes the very fundamental 'misunderstanding' in evaluating the new security environment both Williams and Corpora warn against. In reality, the factors which breed terrorism remain the same as they have always been historically: issues of political, social, economic and security discord. As a result, and echoing the long-standing foreign policy debates between 'interests' and 'values,' political strategy and anti-terrorist policies need to focus on those four timeless factors while reason must be used to expose the false religious precepts that are totted as a justification of terrorism.

Gavin Cameron argues that in contemporary security debates regarding policy formulation, there is an important distinction to be made between WMDs, an issue of scale, and CBRN weapons, an issue of type. However, in the context of terrorism, which is by its very essence a tool of political manipulation, the horror and revulsion surrounding CBRN weapons means that even the threat or possibility of their utilisation provides them with a unique and definitive coercive power. No authority can ignore even the threat of their use if it wants to preserve its legitimacy. Consequently, such weapons remain the ultimate prize for terrorists and the criminals who would trade in them. CBRN weapons, therefore, represent the foremost concern for security forces worldwide and make a well-considered and comprehensive response to this specific threat an absolute necessity.

Michael Dartnell asserts that the new security environment is in fact a post-modern one, a milieu in which power is exerted individually through people's values and beliefs. Ironically, in its purest form, this type of power is what classical realist Hans Morgenthau referred to as "man's control over the minds and actions of other men." This new post-modern reality is facilitated by globalisation and it's predominant feature: information technology. Using IT has given non-state actors power commensurate with that of states, as they use international mediums of communication to exert influence on people anywhere, and consequently the cyber world has emerged as yet another arena of competition for the 'hearts and minds' of the people.

Inevitably, this clash of values creates conflict over what we perceive to be threats, and even confusion over who 'we' actually are. Echoing the debate between Corpora and Williams, Dartnell suggests that the challenge of the new security environment, therefore, is that we must change the way we think about, and more importantly how we address through our policies, challenges to human security in the face of nihilistic and apocalyptic threat actors. In this context, victory will be ideological rather than territorial.

Building on Dartnell's conceptual framework, Gary O'Bright demonstrates that like globalisation itself, the cyber world represents both a strength *and* a weakness to implementing security measures because it is where the conceptual and the physical realms join and interact. The cyber world underscores both our dependence upon information technologies and our growing interdependence with each other because of the global scope of this dependence, a relationship that is by its very nature political. Assets of critical infrastructure therefore represent valuable tools for, as well as targets of, criminals and terrorists in addition to being vehicles for legitimate actors like consumers and governments. As O'Bright describes it, the Canadian government's response to this challenge has been proactive, through recognising and testing new concepts, perspectives and approaches to implementing security. However, illustrating the debate between Corpora and Williams, the all-hazards approach adopted by Canada implicitly accepts the notion of convergence and focuses its efforts of redress upon the issues of activity, creating a convergence of response by authorities to meet the convergence of threat. Issues of enterprise, however, seem left to the purview of politicians alone.

One of the pivotal assumptions by security planners since September 11th has been that cyber attacks against critical infrastructures and IT systems would quickly become the norm, if not in fact the primary target of threat actors. However, as David Mussington argues, this simply has not happened and is very unlikely to do so. In the cyber world, 'activity' and 'enterprise' are practically indistinguishable, however, the distinction itself is an irrelevant one because the power to manipulate comes from the fear of death and destruction. According to Mussington, the cyber world conveys none of these motivations. Thus, echoing Badey's assertions in his chapter, our misguided assumptions about this threat means governments are generating unnecessary and ineffective policies about security and guarding the wrong venues. As was the case prior to 9/11, this wastes precious and finite resources while leaving open other avenues of assault that asymmetric attackers seek to exploit.

Leading off the contemporary case studies section of Part One, Viktoriya Topalova's account of the Chechen crisis is not only particularly prescient, given the recent attacks in Russia and Beslan specifically, but is also a convincing illustration of several of the concepts already discussed. The ongoing Chechen conflict embodies: the convergence of criminal and terrorist groups and their transformation into their corresponding types along with the synergistic effect of undermining legitimate authority; the transformation in traditional hierarchical structures towards more horizontal and networked models by both threat actors and authorities; and most importantly, the dramatic effects that our ideological preconceptions and misconceptions of these issues have upon policy formulation and consequently legitimacy. The principal lesson of Topalova's contribution, however, is that corruption and convergence provides threat actors the ability to overwhelm legitimate institutions and create cracks in the jurisdiction of legitimate authority from which to continue their activities and expand their enterprises. The Russian experience suggests for Western observers that responses which treat only the activities of threat actors without considering their overarching enterprises will be doomed to failure or worse, instigate significantly more challenging problems which may then overwhelm legitimate institutions that otherwise would have been resilient.

The implication of Cynthia Watson's study on the effects of corruption upon democracy in Colombia is that the key to creating the security and legitimate authority needed to practice democracy is to allow the resident civil society to make policies and judgments for themselves in accordance with liberal-democratic tenets, as *they* perceive them. Such participation establishes the authority and stability in which essential services can be provided to the populace, which in turn reinforces legitimacy and allows democracy to flourish in a sustainable and reinforcing praxis. If force or coercion is used to impose political order from above, then legitimacy and the acceptance of authority is sacrificed, allowing the forces of disorder the opportunity to assert themselves and expand their spheres of influence across the levels of analysis; from the local to the systemic. The Colombian case study also illustrates how a lack of jurisdictional integrity and authority, or rather order imposed without local support, creates violent competition between parochial groups who then resort to any means necessary to impose their will, including the employment of terrorist tactics. The insights of this case study has interesting implications for the continuing campaign in Iraq and its forceful implementation of 'procedural democracy.'

Completing the case study section of Part One, John Thompson's review of the Tamil Tigers illustrates the disturbing capability of criminal organisations to transform into terrorist ones and vice versa, and even to be both at once depending on which level of analysis the problem is being examined from. This demonstrates that conventional frameworks for analysing and countering illegitimate actors must be revised if they are to be effective in the new security environment. Policy in the world after 9/11 must be holistic, and simultaneously capable of addressing both the activities and enterprises carried out by threat actors. This highly 'Canadian relevant' case also underscores the contention that gaps in the jurisdiction of legitimate authority and regions of disorder left unchecked can breed stronger, bolder and more dangerous illegitimate actors. The synergy of this growth facilitates threat actors who can then come to rival state actors in power, destabilising the entire system of democratic governance both domestically and systemically.

Beginning the conceptual discussions for Part Two of the monograph, 'Tim' Smith reminds us that if democracy is to survive the consequences of attacks with its liberal values and accountable institutions intact (whether the assault be from threat actors or from our own responses like intelligence-led policing) then the only way to preserve what we are defending is to adhere to established fundamental liberal beliefs and democratic principles, particularly when carrying out security measures. Democracies should not overreact to a sudden demand for security and stampede into measures that contravene those tenets, as this would not only choke off the benefits of democracy and globalisation but also lead to sacrificing the very values legitimate authorities are striving to protect; tenets such as the rule of law and equality, negative freedoms such as liberal safeguards for minorities and positive freedoms such as the democratic right to exercise input into public-policy choices or express dissent. If officials disregard these values in the rush to re-establish security, the democratic model of governance will crumble from within.

Looking at the actual mechanics of countering terrorism, James Smith maintains that a strategic approach to the threat-actor problem is essential. After determining both the purpose and the components of the threat actor's strategy, a counter-strategy can be formulated and implemented. Following Phil Williams' assertions, this would involve identifying the target, determining the 'enterprise' of the threat actor, and then thwarting his 'activities' at every phase of his operations tactically. This agenda requires careful planning, detailed intelligence, and seamless inter-agency coordination such as denoted with the all-hazards approach recommended by Gary O'Bright, but also provides the foremost opportunity to ensure the proposed counter-terrorist strategy adheres to liberal-democratic tenets.

Systemically, such a strategy as proposed by James Smith will involve foreign interventions as democracies seek to close any gaps in authorities' jurisdictions, and diminish the forces of disorder at their own bases. Such 'expeditionary operations' illustrate some of the fundamental questions that a democracy must grapple with in responding to terrorist and criminal agendas. Timothy Lomperis contends that there are really only two ways to go about conducting intervention operations: either directly or indirectly. While the indirect approach may typically be more successful and provide the greatest degree of political flexibility, the direct method is more in keeping with democratic practices because it establishes clear lines of authority and is unavoidably transparent in its implementation. However, the direct approach does not provide the same degree of political manoeuvrability for the government conducting the intervention, and also focuses predominately on military solutions which democracies are seldom eager to support or sustain. This creates the great dilemma for the democratic counter-terrorism practitioner: choosing expediency and guaranteeing results that will preserve the state, or adhering to principles and morays that ensure democratic legitimacy, but which may fail to eradicate the threat.

In his next contribution to the monograph, and the first of the case studies section for Part Two, David Charters points out that Canada has taken extraordinary steps to improve its security apparatus since 9/11, even though Canada itself was not directly attacked. He contends Canadian actions have little to do with Canadian security *per se* and much more to do with Canada's relationship with the United States. As such, Canadian initiatives are not so much a response to the threat actors themselves as they are to the American responses to such challenges. Canada's security measures are designed to achieve only two fundamental goals: keeping the Canada – U.S. border open to trade, and protecting Canadian sovereignty through a traditional policy of 'defence against help.' This reinforces long-standing allegations that Canada's security policies are primarily driven by the needs of its allies and by the desire to preserve the stability of both the domestic and international systems, and only secondarily by the need to deter or contain challenges to Canadian sovereignty.

Jeffery Ross concurs with the principal assertion of Part Two, which is that we must be careful not to overreact to the threats of illegitimate actors or succumb to a pervasive and festering paranoia about our world. This pitfall would in and of itself compromise liberal-democratic values and provoke overreactions to the terrorist threat that would allow 'extremist' elements within our own governments to make inappropriate, if not outright detrimental policy choices thereby upsetting our democratic system. He contends that in America, most Homeland Security actions have been more symbolic than substantive, leaving the U.S. little more safe than before the 9/11 attacks but significantly more fearful and subject to sometimes ludicrous restrictions. Fatigue and complacency from always being on alert is another effect of populist, but not necessarily effective, reactions. To reverse this counter-productive trend requires working more *intelligently* towards security objectives and not necessarily working harder.

The reaction to the "intelligence failures" of 9/11 is a case in point to Ross' contention. As the multitude of recent parliamentary and congressional inquires and hearings have demonstrated in the analytically chaotic aftermath of 9/11, intelligence is of pre-eminent importance to countering terrorism, yet serious flaws have been found in the intelligence apparatus of most Western countries. But Lawrence Cline points out that "quick fixes" will do nothing to correct these flaws, and if imposed without careful consideration of the consequences and their implications, politically motivated alterations may in fact leave democracies more vulnerable to threat actors than they were on the morning of September 11th. The recent attempt to reorganise the American intelligence community may be the best example of how misperception and the need to 'do something' by politicians can lead to flawed decisions and policy, which then go on to make circumstances worse rather than better later on.

Reinforcing the pre-eminence and centrality of the intelligence issue in the new security environment, Peter Gill discusses the relatively new concept of intelligence-led policing. He suggests that from the strategic perspective, this practice is ultimately playing into the reactionary nature of public policy in post-9/11 democracies, and is motivated by the partisan desire of politicians to be seen as 'doing something' for the constituents they represent. He contends the implications of intelligence-led policing, in both its domestic and international connotations, threaten to push us from democracy to "securocracy," and to violate liberal-democratic tenets for expediency. The focus on prevention and disruption to the exclusion of prosecution through due process of the law inches democracies toward that slippery slope of authoritarianism. By upsetting the balance of democratic processes and institutions from within, securitisation may do more to help bring about the threat actor's agenda than the threat actors could do themselves.

Finance and the movement of money is the very lifeblood of both organised crime and terrorism, but also serves as their common weakness. As Trifin Roule illustrates, in stark contrast with the responses of polities worldwide, the finance industry's mechanisms of control remain largely unused and its complex rules un-enforced. This leaves the financial milieu essentially anarchic, and one of the foremost means for restricting threat actors therefore left unexploited. The key to crippling both terrorist and organised criminal enterprises lies in drying up if not confiscating their funds, while also utilising the international finance system as an excellent source of intelligence and venue of control through tracking those funds and their networks. However, only a global and coherently enforced set of regulations, which provides for both accountability and transparency, can provide states the jurisdiction to take advantage of this Achilles' heel on the forces of disorder. As demonstrated by the other case studies in this section, the rule of law is the cornerstone upon which this mechanism is based, and cooperation across the levels of analysis is the key to laying such a foundation and generating a comprehensive jurisdiction of order.

The primary obstacle to such a coherent and cooperative system is competing agendas amongst self-interested actors. International organisations have made and continue to make a measurable contribution to monitoring the forces of disorder at the systemic level, and in mitigating the consequences of their activities down to the local level. Kate Bryden asserts that the International Convention on the Suppression of Financing of Terrorism, a mechanism which has facilitated the multi-national attack on al Qaeda funding, serves as an excellent example of what international organisations can do. However, international agencies must not only be effective, they must also ensure that they remain accountable to those they represent and not lose track of their original purposes by becoming partisan actors. One of the primary vehicles by which to ensure accountability and "focus of purpose," Bryden argues, is to de-politicise the terrorism issue, meaning preventing the issue from becoming a diplomatic bargaining chip. The "faddism" that accompanied responses to 9/11 is an example of this, which some international organisations exploited for their own purposes, such as to expand their budgetary resources. Simply passing ever more legislation or ratifying symbolic agreements rather than enforcing those already in existence is yet another example of politicisation, and offers no value as an end in and of itself.

THE IMPLICATIONS OF THE CHALLENGES AND THE MEANS OF RESPONSE

Collectively, these chapters offer considerable food for thought. They provide a fresh perspective on the challenges to democracy posed by threat actors in the new security environment, and suggest what the appropriate means of response to those challenges might be. It must be recognised that the challenge of the threat actor is in fact an existential one for democracy as a system of governance as they are directing their attacks, whether consciously or not, against the very values and principles of liberal-democracy. The key to their success is to create instability and chaos, out of which they may seize the opportunity to establish an exploitative order of their own choosing. However, more importantly for democracy as a system of governance is that in the escalating savagery of this ancient conflict, there is an appreciable risk that democracies will forget the values and principles they are fighting for in favour of the more emotive campaign of who they are fighting against.

Perhaps the best example of the existential nature of the threat is the targeting of democratic processes and institutions, specifically the emerging campaign against the conducting of elections. That the recent attacks in Russia, Chechnya and in Spain (to say nothing of the ongoing insurgency in Iraq) took place just prior to the holding of elections in these countries is no coincidence. The immediate benefit of staging attacks just prior to an election is either to intimidate voters into not participating, thereby de-legitimising the result, or to coerce them into choosing representatives that are more malleable to the threat actor's agenda. Certainly the '3/11' attacks at *Atocha* station in Madrid were key to the Spanish electorate's voting out of a government that was both unable to protect them and also sympathetic to the unpopular Bush Administration. In addition to casting doubt upon the choices of a democratic country, the election of the new Spanish administration was subsequently instrumental to the removal of Spanish troops from Iraq, who were there supporting a campaign intended to bring democracy to that country. This was a development with profound implications politically and systemically, and with consequences well beyond the confines of the Spanish polity.

Using terror to affect the outcome of the Spanish election was a major victory for the *Jihadist* agenda. However, the damage was in fact much more insidious than simply forcing a change in national policy with international consequences. The credible practice of elections is how the legitimacy of a democracy's authority is affirmed and maintained. Undermining that authority and thereby compromising a government's ability to function effectively, domestically and internationally, also undermines the legitimacy of the concept of democracy itself. By frightening people into electing representatives who would abet the *Jihadists*' agenda, the terrorists compromised the institution of elections and the processes of accountability between electorate and their officials, and thereby damaged the very legitimacy of the government. By consequence, this calls into question the adequacy and resiliency of the democratic system they represent.

The insurgency in Iraq has also put the United States of America in an equally difficult position, again demonstrating the systemic linkage between and the influence of the domestic level upon the international, and their increasingly horizontal interdependence. Whether its decision to launch the war to change Iraq's government was correct or not, the United States now cannot afford to falter in its campaign to bring democracy to Iraq. Should the Americans fail to accomplish their goal, for example because an insurgency prevented the effective exercise of authority by a democratically elected government, then not only their own credibility but also that of democracy as a system of governance would be discredited. The critical assertion that "a single sustainable model for national success: freedom, democracy, and free enterprise" and that "these values of freedom are right and true for every person, in every society" would be shattered. Such a turn of events would have implications not only in the Middle East, but throughout world. The good news seems to be that, by contrast with the events in Spain, the efforts of the Iraqi insurgency has so far failed to derail the democratic process, at least in the short term. But the insurgency has yet to be completely defeated, and so the final outcome in Iraq holds promise but remains disquietingly uncertain.

The key insight here for the analyst is the casual flow of these events, the bottom-up implications of national developments upon the international system. In terms of physical destruction at the domestic level, had an attack of equivalent destruction as that of 9/11 been executed upon a lesser state, such as a middle power like Canada or France, then that state would have likely been neutralised as a democratic entity and paralysed as a functioning polity, reduced to a Somalia-like wasteland of anarchy perhaps for years. However, to further complicate the analysis, while such attacks have profound implications for each individual polity, they also have measurable effects for the international system they comprise and its character as a whole. Had the United States of America succumbed to attack and been eliminated as the global democratic patron and sponsor of the international system, it is most likely that democracy as a mechanism of governance along with its liberal tenets *worldwide* would have been discredited and subsequently abandoned. This is why an attack against the United States by post-modern terrorism or against its institutions by organised criminals is in fact an attack against *all* democracies, and why all democracies and legitimate authorities must therefore respond to this challenge.

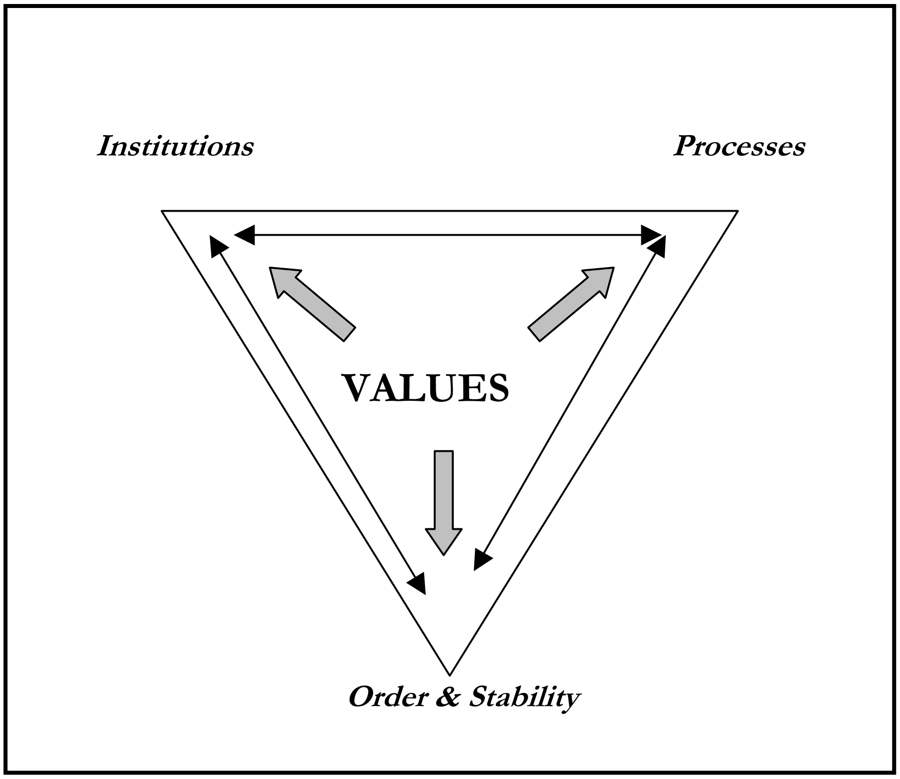
Thus, in the struggle against threat actors, democratic states must act to preserve both their own legitimate polities, institutions and processes, and then also to preserve the larger international environment and system in which those polities exist. So, even if the democratic system of governance is flawed and at times dysfunctional, leaving some to wonder whether or not it is world worth fighting for, as September 11th demonstrated brutally, the world which the post-modern threat actor offers is unquestionably a world worth fighting to avoid. Compelling people to embrace something other than liberal democracy, either to gain respite from constant violence and destruction or through a loss of confidence in their values and way of life, is in reality the true existential threat to democracy.

It is the nature of this existential threat that in fact represents the foremost challenge to democracy posed by terrorism and organised crime, which is that their activities corrupt, subvert and manipulate the very values and principles upon which Western liberal-democracy is based. Whether the threat actor be a petty criminal selling weapons or a terrorist launching asymmetric or even traditional attacks, both the intent and the effect of these activities is to thwart the system and processes which embody and operationalise the values and tenets of liberal-democracy. System and value are inextricably linked by virtue of their being dependent upon, and therefore interdependent *with* each other. For a society to govern itself it must create institutions, and the values of that society are therefore embedded within those institutions it creates. These values and norms by which the society chooses to organise itself are operationalised through the processes by which the established institutions carryout their functions, and those processes can only be carried out legitimately in an orderly and stable environment of acquiescence to authority. This creates a casual chain for democracy that, whether consciously or not, threat actors disrupt with their activities in pursuit of their enterprises.

To phrase this logical construct empirically, there is a casual chain of variables that the threat actor (explicitly by the terrorist and implicitly by the criminal) seeks to disrupt and exploit, a triumvirate of interdependent components which make up 'the democratic dynamic': 1) institutions and 2) processes, balanced upon 3) the foundation of order and stability. The interaction between these delicately balanced components is the means by which democratic values are operationalised and practiced by society. This triumvirate can be visualised as a triangle actively balanced on its point rather than resting upon its base. By launching attacks, either physically or through corruption, the threat actor can disrupt a process and thereby also impact an institution and cause disorder and instability, consequently affecting the resident values of the system. Likewise, an institution can be attacked and its associated processes and values will also be imperilled from the resulting disorder. Interfering with any one of these three variables - institutions, processes and order - by launching attacks or invoking disruption will subsequently affect the other two components to the detriment of the values embedded within the triangle.

Thus, the activities of threat actors can be thought of as trying to knock the triangle off its point onto one of its sides to advance either a political or financial enterprise. Disruptions or changes to any of the variables comprising the triumvirate, either through the physical

Figure 4: The Democratic Dynamic in Balance



destruction of institutions or the abandonment of processes and their embedded values, and the delicate balance of the democratic dynamic is upset thereby knocking the triangle from its point.

The most serious threat to democracy, however, from *Jihadist* terrorism specifically is not that its violence will defeat a democratic state and that its citizens may then rush to embrace to one of its sides. The result of this happening is the transformation of the democratic system to something else, such as authoritarianism or tyranny. an order based on 'divine will.' Rather, the risk is that should such attacks continue successfully, the citizenry of states (and by consequence the international community and the system they comprise) may eventually abandon liberal democracy in search of a system of governance that *can* provide security and stability. In their desire to restore order, constituents would abandon their legitimate institutions with checks and balances and rules, and forego their faith in liberal-democratic values to satisfy their needs, and turn instead to something else that is entirely alien to democracy, such as theological authoritarianism or militarism and tyranny.

The challenge then for policy makers and practitioners is double-sided, as the existential threat comes from not only the attacker but also from the polity responding to the attack. If a government strengthens institutions or curtails processes, the balance of the dynamic is disturbed just as effectively as if a terrorist mounted an attack. Changing the overall nature of this dynamic by upsetting its balance is the win/win scenario for the threat actor: if the government does not do enough to constrain the threat actors then their attacks continue and further erode confidence and legitimacy in the system, while if they do too much the system is unwittingly destabilised and potentially provokes a systemic change from within, as civil society reacts to the changes.

A review of the contributions to Part Two of the monograph indicates that, even more important than the challenges threat actors present to democracies, is the very means by which democracies themselves respond to these challenges as it is their responses that truly define their nature and hence their worth as a just and legitimate system of governance. This is more than 'liberal rhetoric' or 'academic semantics,' as in the new security environment the struggle between governments and threat actors is ultimately an ideological one. This requires both empirical reasoning *and* the emotional and instinctual appeal of 'justice' if liberal democracy is to prevail, not only domestically but on an international scale in terms of the character of the international system. In the final analysis, whether caused by threat actors or by our own governments, disrupting the operationalisation of values between the three variables of the dynamic via altering any of the individual components themselves in this finely balanced triumvirate – institutions, processes, and order operationalising embedded values – will only lead to the emergence of different values from the ones we are trying to protect and consequently birth a *non*-democratic form of government. The risk of such a development is that a more authoritarian or elitist form of government will emerge, one that can at best claim to be democratic in *process* rather than *character*.

There are in fact five distinct ways in which democratic governments can become goaded into reacting regressively against their own best interests and those of the electorates they serve. The first obviously is overreaction. This usually occurs in the immediate aftermath of a major attack, when people are frightened and desperate for safety, and governments are eager to demonstrate their authority and legitimacy by providing security. The overreaction normally takes the form of security measures and 'special powers,' but could also involve abandoning the basic principle of 'minimum force.' Second, and derived from the first, would involve trying to preserve order for prolonged periods through the use of arms. Imposing institutions and processes by coercion, without the consent and endorsement of the electorate, is by definition 'unjust' and therefore illegitimate, leaving at best a democracy of process rather than of character: of appearance rather than fact.

The third mistake democracies can make is to engage in high-profile symbolic activities that are intended to make the constituent audience 'feel better' or generate confidence in their government. Such symbolics are in fact without substance or the ability to actually improve the situation, much less successfully challenge any threat actor's activities or enterprise. Engaging in such symbolics engenders a false sense of security which then may be all too quickly shattered if another attack is launched. This would expose dishonesty on the part of the authorities and is precisely the kind of cynical policy and partisan practice that would erode confidence in liberal democracy as a system of governance.

The fourth mistake is to allow political leaders to become overly fixated on threats as an issue, or rather as the *only* issue. This results in myopia about these specific threats, leaving other and arguably more pressing issues un-addressed or without adequate resources to successfully mitigate them. There is no shortage of these issues, from the economy to social policy, to health and education. An effective, and successful, government will be one that shows it can balance *all* national issues to create an environment of security, one that facilitates both personal liberty and just democracy.

The fifth and final error derives from this myopia of seeing only threats and security issues, which is the formulation and implementation of 'bad' policy. By this we mean the adoption and practice of legislation and measures that serve to create an environment or circumstances that will be expedient for the short term, but in the long term prove more harmful than helpful in the struggle against illegitimacy. This usually arises from demands, in the wake of an incident, to 'do something' and as a result for governments to be seen as doing something. But 'quick fixes' seldom take into account their consequences, or more importantly the broader impact they will wield upon the social environment to follow. This not only wastes finite resources, but may also fail to correct the very challenges it is meant to address, open other avenues of risk, or create unmanageable 'unintended consequences.'

However, by the same token, democratic governments cannot allow themselves to be paralysed into inaction by the fear of doing the 'wrong' thing. There is much that democracies can do to defend themselves, and the chapters in this book provide some sound guidance to those responses based on both experience and insight. The threats to democracy may be taking new forms and means, but there is an abundance of established 'best practices' that will serve not only democracies well, but also those aspiring to be democratic. Indeed, the knowledge collected in this volume suggests that there can be no excuse for governments to act, or fail to act, out of ignorance.

The broad lessons that can be distilled from these chapters include the following: first, establish an informed and carefully considered approach to the challenge before acting; second, employ responses that reflect the values of the liberal-democratic system to be protected; third, adopt policies and responses that will preserve the credibility and legitimacy of responsible authority; and finally, avoid implementing policies that will in the long-term create circumstances worse than those posed by the original challenge.

These four lessons mean, more specifically, that governments and their security forces need to 'think strategically' about countering the threat actor. This strategic vision must inform and regulate the tactics implemented by democracies to confound both the activities *and* the enterprises of threat actors, terrorist and criminal alike. However, that vision must also be informed by the values and principles we seek to protect. As democracy is founded upon civil society, and the acquiescence of the populace to government authority, governments must ensure public support for the initiatives they take. The processes of democratic institutions and their agencies must be completely transparent and clearly communicated, so that the public is aware of both the threat and the response, and is comfortable that both their best interests and also the interests of justice are being served.

In establishing a 'condition of security,' thereby promoting order and stability, governments must also ensure the continued, effective and equitable provision of services to their populaces directly, as that is the very *raison d'etre* of any government and is the foundation for maintaining legitimacy and authority in society. Yet another critical aspect for democracies to consider when responding is to ensure that there are no 'black holes' in the legitimate authority of government, domestically or internationally. This applies to gaps in legal regimes which can be exploited by threat actors and to gaps in the control of jurisdictions, as in 'failed states' like Afghanistan was, where threat actors can take root and flourish to the detriment of the common good.

Finally, when calculating the 'democratic response' to the post-modern threat actor of the new security environment, governments must recognise that resources are not unlimited and not indefinitely sustainable, especially in light of the plethora of other issues besides threat actors that governments must contend with. Proper stewardship and the responsible, measured use of finite and expensive public resources in the battle against illegitimacy and threat actors must be a foremost concern for policy makers and practitioners in trying to be accountable and representative of their constituents. This means specifically guarding against and rooting out the curse of corruption and partisanship, which is a precursor to subversion and facilitates the collapse of the democratic dynamic from within.

To adhere completely and unreservedly to the dictates and demands of liberal-democratic values is the first and most important principle of the democratic response to the new security environment. To ignore this ideal not only abandons our embedded values, undermining the democratic system and mutating it into a regressive form of governance, but also sends the completely unacceptable and unthinkable message that the democratic system itself is not adequate to address the threats of the day and that its values are inferior to those of other systems, such as authoritarianism. As a case in point, this message is implied all to clearly through the grotesque practice of 'renditions' or by using special security certificates, policies which suggest that due process is not capable of collecting intelligence, distributing justice or protecting the constituents of legitimate authority. Even more menacingly, it sends the message that in the struggle against terrorism there are no 'good guys,' no 'right side' and no justice, only the side which is more powerful.

With that in mind, democratic governments must allow, and even facilitate if necessary, meaningful venues and mechanisms of dissent, redress and legitimate opposition to the responses towards threat actors and the means by which they are carried out. They must also encourage, by example if they are to be truly credible, respect for democratic processes and outcomes even if these outcomes are politically or ideologically 'inconvenient.' Stable and just systems of government are constructed from the bottom up, not imposed from above. Like the construction of the ideal system of governance itself, the knowledge required to facilitate that system's construction and administration is iterative and must be undertaken from a holistic and dynamic perspective, and not from the standpoint of aesthetics or ideological rhetoric. As the Pentagon's

Defense Science Board concluded in its 2003 report on the new security environment, "we can never win the global war on terror unless we first win the war of ideas." This legitimacy and democratic order, in turn, must be facilitated by an active and informed public debate regarding security matters and about national policies and goals in general.

The continued questioning and evaluation of new perspectives on old problems, beyond that which is contained in this volume, will be an essential exercise for policy makers and practitioners if the foundation for sound and employable policy so acutely needed in the new security environment is to be derived from the process of reappraisal advocated in these pages. Ultimately, it is more than the answers themselves that we as citizens and participants in our own democracy must consider, we must also strive for wisdom and understanding of these challenges as gained through the process of continuously engaging in analysis and re-evaluation of what we *think* we know. It is the essence of a strong democracy's character that its civil society take the time and effort to examine as many of these perspectives as possible and that we hypothesise about their implications before developing policies because, ultimately, the next security environment will be an environment of our own making. Contributing to this process of reappraisal and ongoing debate is central to the ongoing research agendas of both the *Centre for Conflict Studies* of the University of New Brunswick and the *Centre for Foreign Policy Studies* at Dalhousie University, and has been the foremost objective of this volume.

ENDNOTES

[1] It must be noted at the outset that the interpretations and inferences drawn from the contributor's submissions in this volume for the concluding chapter are those of the editor exclusively, and unless citing a direct quotation from the text may not reflect the views or conclusions of the contributors themselves.

[2] George W. Bush, *National Security Strategy of the United States of America*, September 2002, <http://www.whitehouse.gov/nsc/nss.pdf>, accessed 23 October 2003, p. 3.