Europe, rather than the Middle East and North Africa, if the question is one of the overall strategic importance of the countries targeted to the democracy promoter. This does not invalidate the book's findings about the EU, but might have led to different ones.

When it comes to the US, a couple of Huber's arguments are not entirely convincing. That the Reagan administration used a democracy rhetoric and identity to give a patina to its foreign policy and as a result became entrapped in an actual policy of democracy promotion, alongside being socialized by its Latin American other, may be partly true, but too much importance is given to this relative to other factors. Second, the argument that Reagan initially attempted a return to a *realpolitik* foreign policy but that Carter's experience with human rights meant this was no longer an acceptable option does not convince. Leaving aside the important question of whether Reagan was a *realpolitik* practitioner or not, the extent of his supposed initial abandonment of democracy in Latin America here overestimates the democracy content in Carter's foreign policy. It would be more accurate to say that the change between the two was more a case of different conceptions of the same goal.

Democracy promotion and foreign policy is an important addition to the literature on this subject. Huber's conclusion that, as well as for the United States and the European Union, the identity factor was important for Turkey's decision to move towards a policy of democracy promotion in the 2000s, is an important one. When it comes to considering the prospects for democracy promotion as a feature of international politics, this is a telling contribution to the ongoing debate as to whether non-western democracies would also be willing to adopt such a policy. This book suggests that this cannot be ruled out—but, crucially, that if they do so, it will be in their own particular ways.

Nicolas Bouchet, German Marshall Fund of the United States, Germany

Disruptive power: the crisis of the state in the digital age. By Taylor Owen. New York: Oxford University Press. 2015. 248pp. £12.75. ISBN 978 0 19936 386 5. Available as e-book.

The real cyber war: the political economy of internet freedom. By Shawn M. Powers and Michael Jablonski. Champaign, IL: University of Illinois Press. 2015. 288pp. £50.50. ISBN 978 0 25203 912 6. Available as e-book.

Cyber war versus cyber realities: cyber conflict in the international system. By Brandon Valeriano and Ryan C. Maness. New York: Oxford University Press. 2015. 288pp. £20.00. ISBN 978 0 19020 479 2. Available as e-book.

Unsurprisingly, digital technologies have altered the power balance in international affairs. These three books question this profound, increasing alteration, as well as explain how the internet is redefining diplomacy and our understanding of concepts like sovereignty and territoriality. Today, the internet and its uses have vaulted into the highest realm of 'high politics': the internet has become a venue of unprecedented opportunity, a source of vulnerability, a disturbance in the familiar international order, and it is often portrayed as a potential threat to national security. At the same time, the digital economy spreads a story 'full of promise' that often blinds policy-makers, which raises important questions about how much power should be left in the hands of internet multinationals.

In an accessible book for the general, non-academic reader, Taylor Owen assesses these mutations through a 'disruptive power' lens: empowered by digital technologies, many non-state actors are leveraging their ability to challenge traditional centres of power across a number of areas related to international relations. States now find themselves in a

convoluted position, as both enablers and targets of disruptive actors. The author provides multiple examples of this 'twenty-first century foreign policy challenge' which threatens the institutions that have preserved the balance of power since the end of the Second World War. First, a group like Anonymous is decentralized (there are no gatekeepers), collaborative (as an intrinsically social world based on partnerships, collaborations and interdependencies) and resilient. In a second example, Owen explores digital activism through the case of the hackers group Telecomix, who served in particular as a form of tech support during the Arab Spring in 2011. As conflict began in Syria, Telecomix agents in France, Germany and Sweden disseminated videos and pictures of atrocities committed by Assad's police and military forces. The cluster anticipated an internet shutdown in Syria similar to what happened in Egypt. Instead, the Ba'athist regime monitored the internet and social media activity of rebel groups and activists. In the case of Anonymous, western governments such as the United States and the United Kingdom have launched criminal proceedings against individuals suspected of being connected to the organization. In zealously prosecuting activist hackers, the author argues, 'the state is doing more than breaking its bargain with citizens', concluding that the effort to control the internet could undermine the democratic state by intimidating its citizens and destroying its own character in the process.

Owen also provides readers with a stimulating discussion on the rise of Bitcoin, and what cryptocurrencies mean for the international financial system that states have long controlled. Bitcoin was imagined and conceived as a radical means of opposing state power. While increasing attention is being paid to its practical commercial utility, there is a growing divide in the cryptocurrency community between those who want to normalize its use and those who remain steadfast in their revolutionary beliefs.

Shawn Powers and Michael Jablonski's book will be of particular use to International Relations scholars and readers eager to place global digital issues and debates into their geopolitical and geo-economic contexts. Its central argument rests on the idea that efforts to create a singular, universal internet built on western legal, political and social preferences, alongside the 'freedom to connect', is driven primarily by economic and geopolitical motivations rather than humanitarian and democratic ideals. Until recently, global internet governance was restricted to small silos of experts. The literature on the subject was suffering from an overly narrow, technocratic conception of internet governance and paid insufficient attention to governance dynamics within countries. In other words, the internet cannot be detached from the multiple regional and national contexts in which it operates. Besides, academic studies on internet governance have tended to address two 'tribes' that do not necessarily interact, or even understand each other: foreign policy scholars and internet and computer science experts. Bringing together these fields has proved particularly necessary since Edward Snowden's revelations, which have shown that internet policy has far-reaching implications which go beyond merely technical issues. This is precisely what Powers and Jablonski intend to do in this meticulous book.

Unsurprisingly, US internet policy captures much of their attention; it is dissected in a more rousing way than by Daniel R. McCarthy in his recent *The power and politics of US foreign policy and the internet* (Palgrave, 2015; reviewed in *International Affairs* 91: 3). In short, the US internet industry has become a key priority for the White House, in terms of both economic redevelopment and the country's security strategy. The internet is involved in the containment strategy against China and the isolation of Russia, through control of networks, the definition of international standards, protectionist measures against Chinese equipment, data capture and the conclusion of trans-Atlantic and trans-Pacific trade agreements which exclude these two countries. Moreover, the current institutional system

allows the US to maintain an unprecedented legal influence via the supremacy of its soft law and the English language. Debates over internet governance are—unlike in Europe—monitored at the highest levels in Washington; the careful maintenance of the status quo is necessary in order to avoid a *retournement du monde*. Despite much rhetoric about openness, participation, accountability and democracy, the current governance model—labelled as 'multistakeholder'—is far more participatory than pluralistic, because it is dominated by representatives of commercial and political interests to the detriment of developing countries and the civil society, who are unaware of the stakes or unable to weigh into the debates. Like Owen, Powers and Jablonski raise the significance of understanding the private sector's role in global internet policy. Today, major internet companies' CEOs are welcomed abroad as heads of state; they recognize the borders of disputed territories on their online platforms. Some openly criticize the US government's internet policy. In some way, the role of such private actors is reminiscent of the role played by the East India Company in seventeenth- and eighteenth-century Europe: sometimes an ally, sometimes a rival of states, and indifferent to their laws.

In a comprehensive and sobering book, Brandon Valeriano and Ryan Maness expend the state-centric prism favoured in the other books under review. Many actors from governments, academia and the private sector have strenuously argued that states must agree on a set of international norms for conflict in cyberspace. Our current environment is characterized by a steep rise in the development of offensive cyber tools and tactics—as well as a general disagreement on when and where it is appropriate to use them. The overall result is a popular perception of a weakened international security environment that threatens to devolve into an anarchic Hobbesian world of 'all against all'.

Evidently, the peculiar features of the cyber phenomenon present an intellectual difficulty: how to integrate its new dangers into existing political and strategic understandings. The problem faced by decision-makers is the reverse and graver question: how to adapt and apply outmoded axioms to reduce the risk. These problems of strategy are not unique to our cyber age; earlier generations of thinkers grappled with similar dilemmas during previous technological revolutions, but they are amplified by dangerous conditions of strategic instability in the 'new domain' of the internet: offence dominance, attribution difficulties, volatility in weapons systems and power dispersion.

In the end, cyber policy and global data flows are undoubtedly becoming a key instrument of power alongside oil and financial flows, as these three books skilfully demonstrate.

Julien Nocetti, Institut Français des Relations Internationales, France

Conflict, security and defence*

Explanation and progress in security studies: bridging theoretical divides in International Relations. By Fred Chernoff. Stanford, CA: Stanford University Press. 2014. 328pp. Index. £50.15. ISBN 978 0 80479 226 4. Available as e-book.

At the heart of this book is the question of why there has been so little progress in knowledge about International Relations (IR). Specifically, Fred Chernoff is concerned with the lack of what he terms 'approach-to-consensus'. By this he means the acceptance of some answers and theories as providing better explanations than their alternatives. He wonders

* See also Brandon Valeriano and Ryan C. Maness, *Cyber war versus cyber realities*, pp. 463–5; Scott Gates and Kaushik Roy, *Unconventional warfare in south Asia*, pp. 494–5; and Peter Hennessy and James Jinks, *The silent deep*, pp. 481–2.