1

Introduction: The Cyber Landscape

Abstract: The opening chapter introduces the key debates in the sometimes confused realm of cyber security and cyber warfare. It identifies that a normative narrative is developing that the threat of major cyber warfare is a real and present danger. At the same time, a number of scholars cast doubt on the level and likelihood of the threat, not least because of legal ambiguities over what constitutes an act of war. Debate is complicated by the heavy involvement of military, security and commercial actors in the discussion. An argument is presented that, while cyber-related threats are present in and around modern warfare, the more catastrophic risks of attack may be unlikely at the present time.

In November 2011, an event occurred in the normally peaceful location of Springfield, Illinois, which soon caused a considerable stir in the world’s media. The story was triggered by the failure of a pump at a public water plant, which caused a number of homes in the Springfield area to find themselves without mains water. On investigation, the pump was found to have had a fault in which it had been turning itself off and on again inexplicably, eventually failing. Analysis of the fault traced the problem back to five months previously when evidence was discovered of traffic between a Russian internet protocol (IP) address and the Illinois plant’s Supervisory Control and Data Acquisition (SCADA) system – essentially the plant’s control network, which can be accessed in certain circumstances over the internet to effect remote controls. The fault in the pump seemed to have developed after this initially unidentified connection over the internet from Russia.

The story gained legs when a security commentator, Joe Weiss, who works for a commercial organisation advising utility companies in the US on how to protect themselves from cyber security threats, mentioned in a blog article that the FBI and Department for Homeland Security (DHS) had been investigating the incident and viewed it as a suspicious cyber attack emanating from Russia.

This was enough for media outlets across the world to pick up the story and present it as one of the first verified examples of cyber techniques being used to attack and disable civilian utility networks. Some of the less circumspect news organisations were unequivocal in their analysis. This was clearly an attack by “Russian cyber criminals”, and represented a worrying precedent. When a DHS spokesman said there was no apparent threat to the integrity of public utilities or to public safety, an anonymous online hacker disagreed and claimed to have hacked into the SCADA network of a second public utility in South Houston, Texas.¹

The problem with the story, as was reported reasonably widely a few weeks later, albeit with slightly less attention, was that its whole premise turned out to be erroneous. A contractor at the Illinois plant in question, Jim Mimlitz, revealed that he had watched the hacking story unfold with incredulity. He explained that the origin of the original online traffic from Russia to the water plant’s network was himself. While holidaying in Russia, Mimlitz had been asked to check something at the plant and had done so over an internet connection, inadvertently causing the fault.²