

## Australian Outlook

### In this section

#### Modern Espionage: From Wikileaks to Panama

07 Dec 2020

By Dr Stephen McCombie and Dr Allon J Uhlmann



**The practice of journalism in the twenty-first century has undergone deep transformations. Few people have come to represent these changes as much as Australian Julian Assange. On the tenth anniversary of his arrest, we reflect on how brainchild Wikileaks has carved new paths in cyber journalism.**

Leaking information to journalists is nothing new. However, contemporarily, leaks are substantially easier to execute. In the 1970s, the leak of the Pentagon Papers, Rand's top-secret examination of US involvement in Vietnam, involved photocopying 43 volumes constituting thousands of pages and physically sending them to journalists and politicians. It took many months to copy and then leak. Today, a cyber-leak can be executed and distributed in milliseconds. Massive amounts of data can be easily searched and indexed, and the analysis crowdsourced.

Since its founding in 2006 by Julian Assange and others, Wikileaks has capitalised on new technologies, publishing numerous classified and private materials passed on by insiders or discovered through cyber breaches. Wikileaks often worked independently to distribute and examine these data dumps, but on other occasions worked with traditional media outlets, such as *The New York Times* as in the case of Cablegate.

Whilst Wikileaks might be the most famous clearinghouse for cyber leaks, it is by no means the only one. Many groups that collect and distribute cyber leaks have emerged. In this new reality, the line between journalism and vandalism is blurred, as demonstrated by hacktivist group Anonymous. As well, the boundary between journalism and espionage has blurred, demonstrated when Russian Military Intelligence (GRU) leaked emails from the Democratic National Committee through Wikileaks to the public.

#### Collateral Murder, Afghan War Diaries & Cablegate

The three insider breaches which led to the US charging and arrest of Julian Assange came from US soldier Chelsea Manning, who was serving in Iraq. The most famous showed footage of journalists and bystanders being shot by US helicopter gunships in 2007. The second, which became known as the Afghan War Diaries, included combat reports of US forces in Afghanistan covering the period of 2004-2009. The third was a massive trove of US State Department Cables describing many nations and their governments in surprisingly frank assessments by State Department staff. These revelations, deeply embarrassing for the US Administration, will provide journalists and historians for decades to come with an enormous encyclopaedic collection of insightful revelations.

## **Crowdleaks**

Wikileaks is not alone in seeking to expose the excesses of political power by revealing confidential data to the public. Hacktivist group Anonymous has targeted numerous organisations like the Mormon Church and Sony Pictures for what they believed were efforts at censorship. Some of these hacktivists could draw on their technical skills to successfully confront their adversaries in cyber operations.

Lulzsec were a group of committed Anonymous members who had said technical skills and were prepared to go a little further than most in breaking the law to reveal the secrets of the powerful. Using a website called Crowdleaks, Lulzsec targeted law enforcement and cyber security firms who sought to slight them. In 2010 the CEO of HB Gary General, Aaron Barr, became the target of Lulzsec, who compromised the firm's email system and distributed their email records using Crowdleaks. Amongst many embarrassing emails unearthed were proposals by the firm to orchestrate apparently unlawful cyber operations for private and government entities, including creating fake social media profiles and creating malware to compromise computers. Shortly after the leak Aaron Barr resigned and HB Gary, the parent company, was sold for an undisclosed amount. This is a clear case where journalism and radical direct action converge in what is a growing trend not only in journalism, but also in radical militancy.

## **Snowden**

In 2013, NSA Contractor Edward Snowden collaborated with journalists from *The Guardian* to release over 7900 top-secret National Security Agency (NSA) files that revealed the breathtaking extent of NSA surveillance of foreign and US domestic targets. Their release led to an investigation of the NSA surveillance practices and the shutdown of numerous efforts which were either found unlawful or had approval withdrawn for them by US Congress. Snowden has since fled to Moscow, where he continues to decry the excesses of the surveillance state. While civil libertarians hail him as a model whistle-blower and a hero, senior bureaucrats and intelligence figures have denounced him as a traitor.

## **North Korean Sony hack**

Revealing secrets is not only the work of those dedicated to civil liberties. Even the North Korean regime, arguably embodying the antithesis of civil liberties, found merit in exposing the secrets of its rivals to the public. In 2014, when Sony Pictures produced a satire regarding the assassination of Kim Jong-Un, the rogue state responded with a cyber-attack that shut down and greatly damaged the studios. The hack meant unreleased films and scripts were stolen from Sony computers, as well copious email correspondences. Some of those emails contained extremely embarrassing commentary from executives at Sony, and revealed evidence of secret efforts by the Motion Picture Association of America to lobby the United States International Trade Commission, which was attempting to gain more favourable rules to prevent movie piracy.

## **2016 US Presidential Election**

Described by Michael Hayden as “[T]he most successful covert operation in history,” the hacking of the 2016 US Election was a significant example of the blurring between cyber journalism and information operations. Special prosecutor Robert Mueller's investigation found GRU stole tens of thousands of emails from the Democratic National Committee and Democratic Congressional Campaign Committee. These were dumped through such channels as Wikileaks and proceeded to scandalise the US. The emails

leaked were genuine, and their publication was a classic case of muckraking journalism. The embarrassing revelations forced the resignation of DNC Chair Debbie Wasserman Schultz on the eve of the Democratic convention over which she was to preside. But the greatest damage was to Clinton's credibility amongst Democrats who had supported Bernie Sanders in the primaries, as some of the stolen materials indicated the DNC had worked to undermine Sanders' campaign.

## Panama Papers

In late 2016, the files of offshore law firm, Mossack Fonseca, known as the Panama Papers, were leaked. These revealed systematic international money laundering by many infamous personalities. The data leak saw over 2.6 terabytes of data passed on to journalists. Interpreting this material required a collaborative effort, and the International Consortium of Investigative Journalists coordinated an international group of investigative journalists who pored over the material, collated the documents, and exposed one of the uglier facets of contemporary robber capitalism.

## Conclusion

The emergence of the cyber domain has clearly affected journalism as we know it. More material than ever can be harvested and exposed, either by committed insiders or by malicious outsiders, or even by journalists. Insiders can expect a greater degree of anonymity as they interact with journalists. But this also makes it easier for other actors – such as foreign intelligence agencies – to attempt to control and manipulate journalists. The traditional divide between journalism and espionage has blurred, as has the boundary between the protection of national security, and the cover up of nefarious practices of politicians, tycoons, and bureaucrats. And for setting this new journalistic agenda, few people or organisations can claim more credit than Julian Assange and Wikileaks.

*Dr Stephen McCombie is a senior lecturer in Cyber Security at Macquarie University. His current research interests are in digital forensics, cyber threat intelligence and information warfare. His research draws on a diverse background in policing, security and information technology over the last 30 years. Stephen has also held senior positions in information security with IBM, RSA, National Australia Bank and most recently Secureworks.*

*Dr Allon J Uhlmann is a lecturer in Intelligence Studies and Cyber Security at Macquarie University. He is a social scientist and former public servant with experience in intelligence policy and analysis. He works in the areas of intelligence warfare, cognitive warfare and dynamic information superiority. His main academic teaching covers intelligence theory and practice, strategic surprises, and cyber intelligence.*

*This article is published under a Creative Commons Licence and may be republished with attribution.*

## Related Articles



### Funding Australia's Role in the World

By Jacinta Carroll