Journal of Strategic Security

Volume 15 | Number 3 Article 11

We Are Bellingcat: Global Crime, Online Sleuths, and the Bold Future of News. By Elliot Higgins, New York: Bloomsbury Publishing, 2021.

John P. Sullivan, Ph.D.
University of Southern California, Safe Communities Institute

pp. 138-141

Recommended Citation
Sullivan,, John P. Ph.D.. "We Are Bellingcat: Global Crime, Online Sleuths, and the Bold Future of News. By Elliot Higgins, New York: Bloomsbury Publishing, 2021.." *Journal of Strategic Security* 15, no. 3 (2022) : 138-141.
DOI: https://doi.org/10.5038/1944-0472.15.3.2060
Available at: https://digitalcommons.usf.edu/jss/vol15/iss3/11

We Are Bellingcat: Global Crime, Online Sleuths, and the Bold Future of News. By Elliot Higgins, New York: Bloomsbury Publishing, 2021.

***We Are Bellingcat: Global Crime, Online Sleuths, and the Bold Future of News*. By Elliot Higgins, New York: Bloomsbury Publishing, 2021. ISBN 1635577306. Notes. Index. Hard Cover Pp. 272. Hardcover $13.99.**

Review by Dr. John P. Sullivan

Open source intelligence (OSINT) can be a powerful tool for gaining situational understanding. Social media, imagery (satellite and overhead images such as Google Earth, as well as digital images and videos), together with media reports and mobile phone metadata data can help uncover criminal conspiracies and hybrid warfare campaigns. As government agencies seek to optimize the use of OSINT and its derivative social media intelligence (SOCMINT), Elliot Higgins a citizen journalist, a member of the technical advisory board of the International Criminal Court (ICC) in the Hague, and founder of Bellingcat, an investigative journalism firm (stylized as "bell¿ngcat") recounts the development of his crowd-sourced investigative enterprise in his book *We Are Bellingcat: Global Crime, Online Sleuths, and the Bold Future of News*.

Introduction and Revolution in a Laptop

The saga reads like an adventure story as Higgins—formerly known as the blogger "Brown Jones"—tells the story of Bellingcat's rise. The book covers interesting ground. It is a cross between an organization biography and brief history of the rise of contemporary hybrid warfare. Its introduction begins with a brief account of the 2018 chemical weapon (CW) attacks on Sergei and Yulia Skirpal with Novichok, a Russian class of nerve agents, in Salisbury, England (UK). Novichok agents are a class of weapons prohibited by the Chemical Weapons Convention (CWC) and Organization for the Prevention of Chemical Weapons (OPCW), with tell-tale signatures identifying them as Russian in origin.

The text continues in Chapter 1, "Revolution in a Laptop" where the development of crowd-sources online investigations is described from the early days of the blog *Brown Jones* through the formation of Bellingcat—an enterprise for early warning or "belling the cat." This evolution starts with assessing CW, cluster bomb, and barrel bomb attacks in Syria and the

disinformation surrounding these campaigns. Higgins sums up his early mantra as: "Identify, Verify, and Amplify" to expose atrocities (p. 60).

Becoming Bellingcat

Chapter 2. "Becoming Bellingcat" provides an overview of how digital "detectives" investigated the downing of Malaysia Airline MH17, which was traveling from Kuala Lumpur to Amsterdam, over Ukraine on 17 July 2014. This investigation involved an online investigative community, led by Higgins, to provide a "crowd-sourced" *ad hoc* investigative team. The team employed "geolocation," photo and image analysis, and geospatial information (essentially IMINT and GeoINT) to uncover the "Little Green Men" behind the attack, expose the Russian involvement and diffuse the Russian attempts at misdirection through propaganda. The team provided a detailed timeline and provided expert testimony to the official Joint Investigation Team fielded by the Netherlands, Australia, Belgium, Malaysia, and Ukraine.

Chapter 3. "Firewall of Facts" describes how Bellingcat's efforts to expose the truth were countered by rogue state-sponsored cyberattacks, and *Maskirovka* (Russian "disguise" and counter-influence operations). These efforts to chill disclosure of belligerent acts by Russian agents included "spear-fishing" attempts, disinformation/propaganda by state-sponsored "troll" armies, and the use of alt-media sites promulgating "fake news" to sow confusion and skepticism. These efforts included the deliberate slander of civil defense efforts in Syria by the "White Helmets." These efforts also included false accusations of chemical attacks which Bellingcat discredited.

The overall theme is one of hybrid influence with rogue state actors developing and unleashing lies, and disinformation as part of a global gamification of hate. The result is a counterfactual community comprised of alt-right actors (including) Neo-Nazis, Proud Boys, and terrorists (including ISIS) spewing antisemitism, neofascism, and white supremacist memes as seen in the 2019 attack on a mosque in Christchurch, New Zealand. The manifesto "justifying" this attack was later disseminated broadly in the alt-right counterfactual ecosystem.

https://digitalcommons.usf.edu/jss/vol15/iss3/11
DOI: https://doi.org/10.5038/1944-0472.15.3.2060

Mice Catch Cat and Next Steps

In Chapter 4. "Mice Catch Cat," Higgins returns to provide a detailed after action of the investigation into the attack on the Skirpals in Salisbury. Here, Higgins documents links to the Russian FSB and GRU (Federal Security Service and Main Directorate of the General Staff of the Armed Forces of the Russian Federation). In doing so he meticulously identified the Russian agents and action cell (essentially a murder and subversion team) with ties to GRU Unit 29155 and state CW lab known as "The laboratory." Tools utilized included mobile phone meta-data as part of an emerging digital forensic research practice.

The next steps for digital sleuthing described by Higgins involves the use of Artificial intelligence (AI), including machine learning (ML) and algorithms. These tools will assist online investigators to develop and disseminate verified OSINT on war crimes cases and atrocities. AI will also be used to help states and humanitarian organizations disclose and declaw disinformation by providing the tools for countering deepfakes on synthetic media. Bellingcat is using several means to reach this goal. One of these involves standing up a joint innovation lab in Berlin together with other entities including Forensic Architecture, the Syrian Archive, and the European Center for Constitutional and Human Rights (ECCHR) (p.214). Other efforts include disseminating a *Bellingcat Online Investigative Toolkit*, sponsoring the development of new online digital investigative tools by sponsoring remote global hackathons on network and digital investigation tools, and hosting digital investigative workshops (see *bell¿ngcat* website at https://www.bellingcat.com for current offerings).

Conclusion

OSINT and SOCMINT are important tools in the intelligence armamentarium. While Bellingcat is not the first entity to embrace networked OSINT—the Los Angeles Terrorism Early Warning Group did so, starting in the mid-1990s—it is a prime example of networked collaboration and innovation.[1] Bellingcat embraced and expanded the use of crowd-sourced open source investigations, honed digital forensic skills, and provides insight for intelligence practitioners of all varieties (OSINT, SOCMINT, and All-Source analysts). *We Are Bellingcat* is an excellent overview of the evolution of OSINT as an accepted tool in mass atrocity

investigation. It also provides, an accessible primer in understanding digital forensic investigations for intelligence analysts and decisionmakers in the military, law enforcement, judicial, and humanitarian communities. The book contains notes and an index making its contents accessible for intelligence, counterterrorism, and hybrid threat analysts seeking to explore and enhance their craft. Finally, as David Ronfeldt and John Arquilla have often stated, "It takes a network to [counter] networks."[2] Higgins clearly demonstrates the power of a networked collaborative to counter dark networks, hybrid threats, and atrocities.

---

[1] John P. Sullivan and Alain Bauer, eds., *Terrorism Early Warning: 10 Years of Achievement in Fighting Terrorism and Crime*, (Los Angeles" Los Angeles County Sheriff's Department, October 2008), https://www.academia.edu/1115115/Terrorism_Early_Warning_10_Years_of_Achievement_in_Fighting_Terrorism_and_Crime.

[2] David Ronfeldt and John Arquilla, "Networks, Netwars, and the Fight for the Future," First Monday, Vol. 6, No. 10 (October 2001), https://firstmonday.org/ojs/index.php/fm/article/view/889/798.

https://digitalcommons.usf.edu/jss/vol15/iss3/11
DOI: https://doi.org/10.5038/1944-0472.15.3.2060