Published on *USC Center on Public Diplomacy* (https://uscpublicdiplomacy.org)

Thumbnail Image:

ACKS
ATTACKER
ORGANIZATION
Road Runner
LOCATION
Harker Heights, United
IP
24.243.
7:29.94
unknown, Moldova

Nov 04, 2016 by Shaun Riordan

Cyber Diplomacy vs. Digital Diplomacy: A Terminological Distinction [1]

The debate about diplomacy in the digital age has been recklessly profligate with terminology. Terms such as e-diplomacy, cyber diplomacy or digital diplomacy have been used almost interchangeably, with each author sticking to his/her favorite. This not only wastes three perfectly good terms where one could do (denying us the other two for other purposes). It also conceals considerable confusion about the relationship between diplomacy and the digital world. In particular it tends to conflate two very distinct activities: the use of digital tools to advance diplomatic ends, and the use of diplomatic tools to resolve issues arising in cyberspace. Often heated debates arise because one participant is talking about the first aspect and the other the second. To avoid these confusions and unnecessary debates (we have plenty of necessary debates in these areas) I would like to propose the following definitional distinction: we should use the term "digital diplomacy" to refer to the use of digital tools and techniques to do diplomacy (including consular diplomacy), and we should use the term "cyber diplomacy" to refer to the use of diplomatic tools, and the diplomatic mindset, to resolve issues arising in cyberspace. According to these definitions, both digital diplomacy and cyber diplomacy can be carried out by state and non-state actors, including companies and NGOs. I invite readers to come up with a separate use for the term "e-diplomacy" (which seems to have lost traction recently in comparison with digital diplomacy and cyber diplomacy).

I have written recently on this blog about digital diplomacy. Essentially it is instrumental, rather than an end in itself. Governments, or non-state actors, have objectives they want to secure and develop a diplomatic strategy to secure them. This strategy will include a broad range of tools and techniques, including digital tools. Digital tools can enhance analysis, engagement with key stakeholders and influence key policy debates. They can also support consular diplomacy. Digital tools are not limited to social media (although these can have value, provided they are used strategically) but should also include web-sourced analysis, Big Data, data mining, digital platforms for scenario generation or conflict simulation and gamification (the use of game play for education and shaping policy environments). Major challenges for digital diplomacy include developing digital tools tailor made for the pursuit of diplomatic strategies (rather than depending on commercial off-the-shelf products), creating effective spaces where state and non-state actors can come together to shape key geopolitical debates, and the evolution of diplomacy itself to integrate the future digital natives generation of political leaders.

Using digital tools to promote broader diplomatic agendas and using diplomatic techniques and mindsets

to analyze and manage issues arising in cyberspace are separate, although related, activities. Failure to distinguish clearly between them has led to considerable confusion among both academics and practitioners.

But cyber space does not only offer digital tools for the more effective pursuit of diplomatic strategies. It also generates a whole series of governance and other issues that can benefit from the techniques and mindset of the diplomat. For example, the issue of Internet governance and the role of ICANN has generated a debate drawing in governments, companies and NGOs. The kinds of multilevel and heterogenous coalitions we see emerging resemble those central to other global issues like climate change. The skills and mindset needed to construct and sustain such coalitions are essentially diplomatic. It is similar with cybersecurity. While most companies still depend on technical and perimeter oriented defense, the development of broader, more forward focused diplomatic strategies can reinforce technical cybersecurity through the identification and dissuasion of potential hackers, the promotion of collaboration between governments, companies and other key stakeholders, convincing public opinion of the guilt of hackers rather than companies and enhanced collaborative working, whether within companies (silo busting) or along supply chains.

Using digital tools to promote broader diplomatic agendas and using diplomatic techniques and mindsets to analyze and manage issues arising in cyberspace are separate, although related, activities. Failure to distinguish clearly between them has led to considerable confusion among both academics and practitioners. The terminological distinction suggested in this blog offers the prospect of greater clarity. According to the definitions offered here, digital diplomacy and cyber diplomacy can be carried out by both state and non- state actors (including companies and NGOs), but they are very distinct kinds of activities.

Photo by Bill Smith | CC BY 2.0