Proceedings of the Weizenbaum Conference 2021

Democracy in Flux

Order, Dynamic and Voices in Digital Public Spheres

Public Opinion and its Influence on Cyber Crisis Decision-Making Processes

Burgers, Tobias
Cyber Civilization Research Center,
Keio University
Tokyo, Japan
burgers@keio.jp

Farber, David
Cyber Civilization Research Center,
Keio University
Tokyo, Japan
farber@keio.jp

KEYWORDS

Cyber Conflict; Public Opinion; Society-centric Conflict

DOI: 10.34669/wi.cp/3.4

The proceedings of the Weizenbaum Conference 2021 "Democracy in Flux: Order, Dynamic and Voices in Digital Public Spheres" have been funded by the Federal Ministry of Education and Research of Germany (BMBF) (grant no.: 16DII121, 16DII122, 16DII123, 16DII124, 16DII125, 16DII126, 16DII127, 16DII128 – "Deutsches Internet-Institut").

Cyber incidents have undergone an escalatory trajectory in recent years. In the quantitative dimension, we have noticed an increase in cyber-attacks. Meanwhile, the qualitative impact of cyber-attacks has increased. It is not solely a game of information theft anymore: Actors are using cyber means to destroy targets in the digital realm and increasingly the physical realm in particular targets that are part of critical civilian infrastructures, such as electronic grids, dams, and harbors (Burgers and Farber, 2021). We observe the rise of what we refer to as *societal-level cyber-attacks*: Cyberattacks, targeting critical civilian infrastructure, whose impact is foremost noticed by civilians and which the blur lines between the civilian and military domain. This is part of a larger development in which the civilian domain is becoming increasingly part of the (military) conflict domain. To paraphrase Zac Rogers (2019) "populations, not soldiers, are now on the front lines."

If populations are becoming part of a conflict, the frontline even, we argue it is imperative to understand the societal dimension of cyber conflict. If societal-level cyber-attacks turn cyber conflict into a society-centric conflict, it seems imperative that we understand what Levite and Shimshoni (2018) refer to as the social dimension. In their essay, the authors illustrate the importance of the public and its role in society-centric conflict (Ibid, 2018). As such, we argue we must develop an understanding of what we refer to as *society-centric cyber conflict* (Burgers and Farber, 2021). Rovner (2021) illustrates how to date, a limited understanding of how societies could react to such cyber-attacks exists. What happens if society becomes subject to possible blackout and lapses in social order due to cyber-attacks? Rovner (2021) argues that societies could pressure their political leadership to seek a settlement with the attackers. However, what if populations react the opposite way, and demand a robust and forceful response, possibly even with conventional military means against an adversary? To date, due to the absence of hard data, it remains speculation how societies would react and how their reactions could shape the question of how political national-level leadership would react to societal-level cyber-attacks.

What is clear, however, is that those cyberattacks are increasingly becoming a pressing issue for societies. Polling by institutions, such as the Pew Center, has illustrated that cyber threats are increasingly on the broader public's radar. In Japan, which we are based, a 2018 survey by Pew Center illustrated that 81% of the respondents view cyber threats as the top security threat (Poushter, J. and C. Huang, 2019). Respondents in other nations, such as the Netherlands, South Africa, and the United States, mark cyber threats as their primary threat, albeit with lesser percentages. These numbers illustrate a significant public fear of cyber threats and -conflict. However, beyond this broader perception, we have limited detailed understanding of how the public would react to a high impact, high visibility societal-level cyber-attacks, which would cause (national security) crises.

It is important to research further the public's perception and opinion on societal-level cyber-attacks. In particular, how the public would react and demand their respective governments to react against the perceived attackers. As Klarevas (2002) illustrates, governmental reactions and the decision-making processes on how to react are influenced by public opinion (Klarevas, 2002). Foremost in democratic nations. Prior high-impact, high-visibility national security events that had a significant societal impact, such as 9/11, have illustrated that public opinion could favor and possibly demand even retaliation, at times even demanding escalatory responses from its government. Such raises the question if such is likely to in the case of successful societal-level cyber-attacks also? In particular, the absence of established protocols, rules, norms, and red lines increases the value of public opinion in the decision-making process (Kreps & Das, 2017). In this, our research builds further on the work of Kreps and Das (2017), as well as another survey we ran prior, which reaffirmed the need for detailed research on understanding how the public perceives societal-level cyber threats and how they would react against such threats.

We are especially interested in understanding if and how the public's reaction could spur the government to react in an escalatory way. The argument that the public plays a role of significant importance in potential escalation and the decision to escalate a conflict, and go to war, is best illustrated by Howard (1979). In his famed essay "The Forgotten Dimensions of Strategy," Howard illustrated the importance of social-political dynamics and public opinions on escalatory behavior and patterns and military conflict (Howard, 1979). While Howard focused on potential nuclear conflict and escalation to military conflict in the nuclear era, we argue that his argument can, and should be, be extended to the current situation also. With societal-level cyber-attacks having a similar effect, impact, and consequences as Howard's conventional military conflict dynamics, it seems equally apt to extend his argument on the public's role and importance of escalatory behavior. Omitting the public's perception and reaction from consideration on the escalation potential of societal-level cyber conflict would omit an essential variable in this process. Howard argued that the "compliance with […] public opinion became an essential element in the conduct of war" (Howard, 1979, p.977). In our opinion, such was the case in 1978, and such is the case today also.

To understand the public's perception and reaction towards societal-level cyber threats and attacks, we conducted surveys in both Japan, South Korea, and Taiwan – a region we believe remains under-researched in the debate on cyber conflict. In our survey, we asked respondents to respond to fictive societal-level cyber attacks and rank their responses. This survey produced exciting and unexpected insights, which we will share in our paper and at this conference. The insights gave an us a first understanding if, how, and by what means the public would like to see a governmental reaction. The sum of this enabled to gain us a better understanding to which extent the public's role in determining governmental responses to societal-level cyber-attacks is escalatory or de-escalatory.

REFERENCES

1. Burgers, T. J., & Farber, D. J. (2021). *Society-centric cyber conflict and the public's role and influence in the escalation potential of societal-level cyber-attacks*, CCRC/KGRI Working Paper Series, Keio University (forthcoming)
2. Howard, M. (1979). The Forgotten Dimensions of Strategy. *Foreign Affairs*, *57*(5), 975. https://doi.org/10.2307/20040266
3. Klarevas, L. (2002). The "Essential Domino" of Military Operations: American Public Opinion and the Use of Force. *International Studies Perspectives*, *3*(4), 417–437. https://doi.org/10.1111/1528-3577.t01-1-00107
4. Kreps, S., & Das, D. (2017). Warring from the virtual to the real: Assessing the public's threshold for war over cyber security. *Research & Politics*, *4*(2), 205316801771593. https://doi.org/10.1177/2053168017715930
5. Levite, A. E., & Shimshoni, J. (Y. (2018). The Strategic Challenge of Society-centric Warfare. *Survival*, *60*(6), 91–118. https://doi.org/10.1080/00396338.2018.1542806
6. Poushter, J. and C. Huang, 2019: *Climate Change Still Seen as the Top Global Threat, but Cyberattacks a Rising Concern*. Pew Research Center
7. Rogers, Z. (2019, June 4). *Have Strategists Drunk the "AI Race" Kool-Aid?* War on the Rocks. https://warontherocks.com/2019/06/have-strategists-drunk-the-ai-race-kool-aid/
8. Rovner, J. (2021, March 17). *Warfighting in Cyberspace*. War on the Rocks. https://warontherocks.com/2021/03/warfighting-in-cyberspace/