Interview – Miguel Alberto Gomez

https://www.e-ir.info/2024/05/14/interview-miguel-alberto-gomez/

E-INTERNATIONAL RELATIONS, MAY 14 2024

Dr. Miguel Alberto Gomez (Ph.D.) currently serves as a Senior Research Fellow at the Centre on Asia and Globalisation (CAG) at the Lee Kuan Yew School of Public Policy (LKYSPP) in Singapore, following a previous role as a Senior Researcher at the Center for Security Studies (CSS) at the Swiss Federal Institute of Technology (ETH) in Zurich, Switzerland. His research focuses on the intricate relationship between emerging technologies, national security, and decision-making processes, with a particular interest in how policymakers utilize cyberspace technologies to serve national interests and their impact on public opinion. His work has been published in well regarded outlets such as *International Studies Quarterly*, *European Journal of International Security*, and *International Interactions*. Dr. Gomez earned his doctorate in Political Science from the *Universität Hildesheim* in Germany and a master's degree in International Security from the *Institut Barcelona d'Estudis Internacionals* in Spain. Prior to his academic pursuits, he spent eight years as an information security professional, following his bachelor's degree in Computer Science from the De La Salle University in Manila, Philippines.

Where do you see the most exciting research/debates happening in your field?

Two promising areas of research in the field of cyber conflict studies in recent years are (1) the increasing interest in its micro-foundational aspects as well as (2) the regional characteristics of cyber conflict. The former refers to growing scholarly inquiry surrounding the cognitive and emotional dimensions of the phenomena. I find this especially important as it brings humans back into the conversation and challenges the technological determinism that characterizes much of the literature. Furthermore, with the lines between cyber conflict and influence operations being continually blurred, as well as the appearance of effects-based operations (i.e., malicious behavior in cyberspace that generates physical effects), it becomes necessary to bring the individual back into the conversation – both elites and the public.

As for the latter, a new generation of scholars at the tail-end of their doctoral studies and a handful of established academics are beginning to shed light on cyber conflict outside the usual North American and European environment. This pivot towards other regions is necessary to provide a broader perspective on the nature of cyber conflict and how best to address it. Moreover, it highlights how middle powers approach cyberspace while keeping in mind their interests and capabilities.

How has the way you understand the world changed over time, and what (or who) prompted the most significant shifts in your thinking?

This was due to shifts in my professional life and the perspectives of those with whom I continue to work (i.e., my co-authors and the broader cyber community). International politics was not my "natural environment" so to speak. I began my career as a cybersecurity practitioner with a Bachelor's Degree in Computer Science before moving to international politics and security. A motivation behind this career change and my subsequent thinking was how cyber capabilities and operations appeared to occur hand in hand with the South China Sea dispute involving the Philippines (I am a national) and China.

Once down this path, the individuals and institutes I worked with shaped my thoughts surrounding the strategic use of these technologies. Around 2016, it was clear that cyberspace was being used as an instrument of statecraft.

Nevertheless, very little was said about how individual decision-makers and the public thought about the domain. This is unsurprising given the underlying assumption of rationality framed the existing theories around cybersecurity specifically and emerging technologies like artificial intelligence broadly. I found this problematic since these technologies are ultimately just tools. How they are used and the subsequent strategic benefits, if any, remained a function of how the users and intended targets viewed them.

From then on, my approach towards international politics tends to put the individual at the center. This is not to say that meso- (e.g., the defense establishment) or macro-level (e.g., the international system) factors do not matter – only that a holistic perspective is required to explain better how states employ emergent technologies that introduce a significant amount of uncertainty into the decision-making process.

How would you best describe the interplay between cyberspace and international politics? Why has cyber-security so quickly risen to the forefront of international political priorities?

Concisely, cyberspace is one enabler of international politics. It might be a bit of a cliché to argue that societal dependence on cyberspace and its constituent parts drives interest in cybersecurity, but this reflects the reality of the modern world. From economic processes to military operations, cyberspace supports the traditional levers of state power. The latent vulnerability of this environment means that state interests can be put at risk. However, the extent to which actors, state and non-state alike, may gain a strategic benefit from this is still up for debate. Nevertheless, this has not prevented malicious actors from engaging in disruptive and degradative behavior that has grown in sophistication in recent years. When viewed alongside persistent hyperbolic depictions from the media about the consequences of cybersecurity incidents, the interest around cybersecurity then becomes unsurprising.

In your paper Trust at Risk you highlight how the psychological impact of cyber-attacks differs greatly from conventional violence. What are the most significant differences in the dynamics of cyber-attacks?

A fundamental difference between conventional violence and cyber incidents is the absence of physical effects. Granted, some of the more prominent cybersecurity incidents in recent years are reported to have resulted in the loss of life, specifically ransomware affecting hospitals. These are not necessarily representative of cyber conflict.

First, it is difficult to prove that the consequences of a cybersecurity incident (e.g., death) are the direct result of a cyber operation. Compared to conventional violence, the link between explosives causing the death of several individuals is quite clear. For cyberspace, this can be second or even third-order effects where a failure of processes due to the loss of digital assets leads to physical harm.

Second, the immateriality of cyberspace means that observing the effects of most cyber incidents is challenging. Someone “hacking” a system does not say much unless an individual is somehow affected by this (e.g., losing access to their account). This leaves a lot to the imagination that is often influenced by what we see in the popular media. Films and shows such as Die Hard 4, Mr. Robot, or Tehran give a skewed picture of how these operations occur and their effects. Unlike conventional violence where the effects are straightforward (e.g., a bomb dropped on a building will level or significantly damage it), there is a significant amount of uncertainty.

Finally, and related to the previous points, the public lacks cybersecurity expertise. This is important as limited understanding prompts the intended or unintended use of specific cognitive and emotional mechanisms that could lead to a distorted view of the consequences of cybersecurity incidents. This is not to say that conventional violence is immune to such, only that the uncertainty brought about by the lack of expertise makes individuals especially prone to this when discussing events involving cyberspace. Fundamentally, the dynamics we see in cyberspace could also occur when we look at more conventional forms of violence. However, variations in how and the frequency in which these manifest differ owing to the unique characteristics of cyberspace.

Your research also postulates that physical distance from the epicenter of a cyber-attack amplifies the adverse effects of the attacks, with political trust conversely highest among those closer to the attack. How should government responses incorporate this new paradigm to better manage public sentiment

and confidence following a cyber-attack?

It might be easier said than done, but greater transparency from the government goes a long way towards building trust following a cybersecurity incident. In the paper, we explain that this effect is due to the ability of those closer to the epicenter of the incident to observe the (limited) effects. As you move farther away, a lack of first-hand experience leads to an overreliance on beliefs that may not accurately capture the realities on the ground. Consequently, governments should get ahead of this and inform the public, within reason, of what happened, what the event's consequences were, and how it affects them.

To what extent has public reaction to cyber incidents matured along with growth in digital literacy? What are the most influential factors which determine how a society will perceive and respond to cyber threats?

Without large-scale longitudinal studies, it is challenging to say with any certainty how the growth of digital literacy influences reactions to cybersecurity incidents. Nevertheless, the available body of knowledge points to the tempering effects of domain expertise (i.e., familiarity with cyberspace) on how individuals respond to cybersecurity incidents. The more a person knows about what cyberspace can and cannot achieve, the more objective their assessments are of cybersecurity incidents.

This is important as it allows one to overcome many misperceptions surrounding cybersecurity incidents and conflict. Specifically, cybersecurity knowledge among policy elites and the public minimizes dependence on stereotypical thinking often grounded on pop culture references. From a societal perspective, this is crucial as it could influence preferences when responding to cyber threats.

Besides their working knowledge of the technology, embeddedness and use are equally important. It wouldn't be a stretch to argue that the more society depends on technologies such as cyberspace for their day-to-day life, the more emotionally salient disruptions to the said technologies become. In this case, it is not the dependence or use of cyberspace that matters but how governments respond to incidents when they occur. Transparency then becomes essential in limiting negative emotions' effect on public preference. The more information the public is given within reason, the less likely their preferences are determined by bias driven by cognitive or emotional processes.

Cross-national war games provide a unique opportunity to observe the intricacies of complex decision-making between multiple states. What exactly are cyber-orientated war games? What do states ultimately hope to achieve and understand by participating in them?

These are simulations such as wargames or tabletop exercises (TTX) that focus explicitly on cybersecurity. From a methodological perspective, simulations as a research method have enjoyed a lot of attention from a growing number of academics over the last five to ten years. This is a response to (1) the challenges often associated with studying elite decision-making and (2) the limitations posed by experimental research.

In terms of the former, many questions international relations scholars are interested in will often center on crisis decision-making. However, the sensitive nature of these events frequently means that much of the information we require is currently classified. To overcome this problem, simulations are a valuable tool that allows researchers to observe and understand how elites or appropriate proxies respond to a simulated crisis. One could say that this is one workaround for the sparsity of data that a lot of research faces. Moreover, this also allows us to complement existing experimental research in that it provides a richness in the data often sacrificed by experiments in favor of generalizability and parsimony.

Concerning cyber conflict scholarship, simulations' growing popularity allows us to unpack better how decision-makers approach this novel technology in an ongoing crisis. Its specific benefits will enable scholars and policymakers to test existing theoretical assumptions surrounding how states utilize cyberspace when pursuing strategic objectives. In my research, these activities highlight how established practices and worldviews often color how decision-makers approach cybersecurity. This, in turn, partially explains the variation in national cyber strategies between states despite facing comparable technological and strategic conditions.

Your paper Breaking the Myth of Cyber Doom you present evidence that sensitivity to digital threats to the polity is grounded on personal threat sensitivity. What factors matter most to people when assessing their own personal threat sensitivity? Is personal threat sensitivity a reasonable measurement of threats to the polity?

Personal threat sensitivity can be operationalized in several ways. For cyber conflict research, this will often focus on (1) physical security, (2) economic security, (3) and/or personal values but could vary depending on the research team. Which factor matters most would vary in terms of context. For instance, individuals who depend on cyberspace as a source of income would be more concerned than those less dependent. Similarly, those who view cyberspace as promoting specific values (e.g., free speech) may be more concerned with censorship than others. Consequently, "what matters the most" will vary and must be evaluated case-by-case.

It is also necessary to note that using personal threat sensitivity to measure threat to a polity is unwieldy since not everyone values the same thing. For this reason, the argument that increasing dependence on cyberspace results in more significant cyber-based conflict rests on shaky ground, as not all societies invest in these technologies at the same level. Personal threat sensitivity is a good starting point but should also be complemented with other measures.

Is the normalisation of cyber threats by the public a positive thing for safer cyber-security? What are the most important factors in maintaining a secure digital environment for societies?

Normative evaluations of whether this is a "good" or "bad" thing are problematic. One could say that normalization is, to a degree, to be expected, given how much modern society depends on cyberspace. This could be a positive or negative development. Normalization could lead to a positive development in that individuals, aware of threats, consciously pursue choices that improve the state of cybersecurity. Inversely, normalization could also bring about complacency in that, seeing the limited impact of cybersecurity incidents, individuals and societies may be less willing to engage in costly exercises to secure cyberspace.

Moving this in a positive direction requires a whole-of-nation approach wherein the relevant actors pursue activities to secure cyberspace within the bounds of their powers. For instance, governments must continue to develop and update regulations and legislation responsive to a dynamic security environment while providing technical and educational resources to organizations and the public. The private sector, particularly the technology industry, should endeavor to institute secure practices in designing, developing, and supporting their products. Finally, individuals should take the necessary steps to secure themselves through proper and safe practices online. While these points are not new, the current state of cybersecurity makes it essential to remind the relevant actors. It is also worth noting that the international community has a role. Specifically, areas of cooperation would include information sharing and confidence building, which prove crucial in addressing cross-border cyber threats. Relatedly, the effort to establish norms of cyber behavior requires states to cooperate and continuously engage with one another in venues such as the UN.

What is the most important advice you could give to young scholars of International Politics?

Young and early-career scholars should keep three things in mind, especially if they are interested in cybersecurity and emerging technologies as an area of study. The first is to avoid disciplinary silos. While there are good professional reasons to work in a specific field, studying technology and its effects on international politics requires us to wear several hats. This advice should not be taken to mean that we should not specialize. Instead, it should be interpreted as a call to learn as much as possible from those in related and tangential fields, as this provides a holistic view of the phenomena. Second, avoid getting drawn into the hype. Those starting should not focus on a specific technology simply because it is the "flavor of the week". Instead, asking how this technology interacts with our understanding of international politics instead of addressing how it "revolutionizes" everything is a more sustainable mindset.

Lastly, and precisely when it comes to the study of technology, insisting on a practitioner-theorist-divide is counterproductive. While there, unfortunately, is a tendency for some to see academic research as more attractive than, say, think tank work, this is a problematic pathology. The inherently applied nature of technologies such as cyberspace and artificial intelligence means we cannot divorce ourselves from how these are employed outside of theory. As such, engaging with those involved with these technologies at a more immediate policy level provides academics with a unique opportunity to broaden their understanding and come up with novel ideas that they may not have thought about otherwise.